Longitudinal study of the cyber norm development process - Cyber Norm Codes

ID	Document	Document Groups	Quotation Content	Codes
2:3	UN GGE - ICT Overview		State efforts to address the security of ICTs must go hand-in-hand with respect for human rights and fundamental freedoms	HUMAN RIGHTS for: respecting human rights and fundamental freedoms; applying them to cyber space / ICT use, etc.
2:4	UN GGE - ICT Overview		States must not use proxies to commit internationally wrongful acts and must ensurethat their territories are not used by non-State actors for unlawful use of ICTs	CYBER ATTACKS disagreement: invoking countermeasures in response to cyber attacks INTERNATIONAL LAW disagreement: the right of self-defense
2:5	UN GGE - ICT Overview		States must not use proxies to commit internationally wrongful acts and must ensurethat their territories are not used by non-State actors for unlawful use of ICTs.	CYBER ATTACKS against: using proxies for [international] wrongful cyber acts
2:7	UN GGE - ICT Overview		In their use of ICTs, States must observe, among other principles of international law, State sovereignty, the settlement of disputes by peaceful means, and non-intervention in the internal affairs of other States	CYBER ATTACKS disagreement: invoking countermeasures in response to cyber attacks INTERNATIONAL LAW for: applicability of international law to cyberspace STATE SOVEREIGNTY for: state sovereignty applied to State's ICT activities & ICT infrastructure within their territory
2:9	UN GGE - ICT Overview		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	CYBER ATTACKS against: using proxies for [international] wrongful cyber acts STATE RESPONSIBILITY & SOVEREIGNTY against: allowing non-State actors in their territories to unlawfully use ICT
2:10	UN GGE - ICT Overview		The UN should play a leading role in promoting dialogue on the security of ICTs in their use by States, and in developing common understandings on the application of international law and norms, rules and principles for responsible State behaviour	STATE RESPONSIBILITY for: dialogue amongst nations by an international body
3:1	2014 - 2015 - UN GGE 2015 ICT re: International Security	2014	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	CYBER STABILITY for: protecting the public core of the internet
3:2	2014 - 2015 - UN GGE 2015 ICT re: International Security	2014	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	CYBER ATTACKS disagreement: invoking countermeasures in response to cyber attacks INTERNATIONAL LAW disagreement: the right of self-defense
3:3	2014 - 2015 - UN GGE 2015 ICT re: International Security	2014	States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs;	INTERNATIONAL LAW for: applicability of international law to cyberspace
3:4	2014 - 2015 - UN GGE 2015 ICT re: International Security	2014	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.	INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information
3:6	2014 - 2015 - UN GGE 2015 ICT re: International Security	2014	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;	HUMAN RIGHTS for: respecting human rights and fundamental freedoms; applying them to cyber space / ICT use, etc.
3:7	2014 - 2015 - UN GGE 2015 ICT re: International Security	2014	States should cooperate in developing and applying measures to increase stability and security in the use of ICTs	CYBER STABILITY for: protecting the public core of the internet
3:8	2014 - 2015 - UN GGE 2015 ICT re: International Security	2014	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;	CRITICAL INFRASTRUCTURE against: knowingly damaging critical infrastructure
3:9	2014 - 2015 - UN GGE 2015 ICT re: International Security	2014	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;	CRITICAL INFRASTRUCTURE for: protecting critical infrastructures
3:10	2014 - 2015 - UN GGE 2015 ICT re: International Security	2014	States should respond to appropriate requests for assistance by another State whose critical infrastructure is subject to malicious ICT acts.	CYBER ATTACKS for: responding to requests for help in the event of a cyber attack
3:11	2014 - 2015 - UN GGE 2015 ICT re: International Security	2014	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;	CRITICAL INFRASTRUCTURE for: protecting critical infrastructures STATE RESPONSIBILITY & SOVEREIGNTY against: allowing non-State actors in their territories to unlawfully use ICT
3:13	2014 - 2015 - UN GGE 2015 ICT re: International Security	2014	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.	CYBER ATTACKS against: targeting emergency response teams
3:14	2014 - 2015 - UN GGE 2015 ICT re: International Security	2014	The identification of appropriate points of contact at the policy and technical levels to address serious ICT incidents and the creation of a directory of such contacts;	CONFIDENCE BUILDING CBM: address issues [related to cyber space/cybersecurity/ICTs]

ID	Document	Document Groups	Quotation Content	Codes
3:16	2014 - 2015 - UN GGE 2015 ICT re: International Security	2014	Encouraging, on a voluntary basis, transparency at the bilateral, subregional, regional and multilateral levels, as appropriate, to increase confidence and inform future work.	CONFIDENCE BUILDING CBM: voluntary transparency
3:18	2014 - 2015 - UN GGE 2015 ICT re: International Security	2014	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.	CRITICAL INFRASTRUCTURE for: protecting critical infrastructures
3:19	2014 - 2015 - UN GGE 2015 ICT re: International Security	2014	A repository of national laws and policies for the protection of data and ICT-enabled infrastructure	STATE RESPONSIBILITY CBM: repository of national laws/policies for data protection and ICT infrastructure
3:20	2014 - 2015 - UN GGE 2015 ICT re: International Security	2014	the publication of materials deemed appropriate for distribution on these national laws and policies;	CONFIDENCE BUILDING CBM: voluntary transparency TRANSPARENCY CBM: publication of materials deemed appropriate for distribution on national laws/policies
3:21	2014 - 2015 - UN GGE 2015 ICT re: International Security	2014	The development of mechanisms and processes for bilateral, subregional, regional and multilateral consultations on the protection of ICT-enabled critical infrastructure	CRITICAL INFRASTRUCTURE for: protecting critical infrastructures STATE RESPONSIBILITY CBM: transnational consulting to reduce risk of misperception, escalation, and conflict
3:22	2014 - 2015 - UN GGE 2015 ICT re: International Security	2014	The development on a bilateral, subregional, regional and multilateral basis of technical, legal and diplomatic mechanisms to address ICT -related requests;	CONFIDENCE BUILDING CBM: address issues [related to cyber space/cybersecurity/ICTs]
3:23	2014 - 2015 - UN GGE 2015 ICT re: International Security	2014	The adoption of voluntary national arrangements to classify ICT incidents in terms of the scale and seriousness of the incident, for the purpose of facilitating the exchange of information on incidents	CONFIDENCE BUILDING CBM: classification/categorization of ICT incidents CONFIDENCE BUILDING CBM: voluntary transparency
3:24	2014 - 2015 - UN GGE 2015 ICT re: International Security	2014	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	INFORMATION EXCHANGE CBM: encouraging exchanges between research and academic institutions STAKEHOLDER COOPERATION CBM: exchange of personnel
3:26	2014 - 2015 - UN GGE 2015 ICT re: International Security	2014	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.	EMERGENCY RESPONSE CBM: each state/regional partnership should establish and/or strengthen a national computer emergency response team (CERT) / cybersecurity incident response team
3:28	2014 - 2015 - UN GGE 2015 ICT re: International Security	2014	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;	STAKEHOLDER COOPERATION CBM: states should support/facilitate cooperation amongst national response teams and other relevant entities
3:29	2014 - 2015 - UN GGE 2015 ICT re: International Security	2014	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	CONFIDENCE BUILDING CBM: address issues [related to cyber space/cybersecurity/ICTs]
3:30	2014 - 2015 - UN GGE 2015 ICT re: International Security	2014	Providing assistance to build capacity in the area of ICT security is also essential for international security, by improving the capacity of States for cooperation and collective action. The Group agreed that capacity-building measures should seek to promote the use of ICTs for peaceful purposes	CONFIDENCE BUILDING CBM: promote the use of ICTs for peaceful purposes
3:32	2014 - 2015 - UN GGE 2015 ICT re: International Security	2014	Assist in strengthening cooperative mechanisms with national computer emergency response teams and other authorized bodies	EMERGENCY RESPONSE CBM: assist in strengthening cooperation amongst national computer ER teams etc.
3:33	2014 - 2015 - UN GGE 2015 ICT re: International Security	2014	Provide assistance and training to developing countries to improve security in the use of ICTs, including critical infrastructure, and exchange legal and administrative best practices;	ASSISTANCE CBM: provide assistance and training to developing countries to improve cybsecurity and ICT use CRITICAL INFRASTRUCTURE for: protecting critical infrastructures
3:34	2014 - 2015 - UN GGE 2015 ICT re: International Security	2014	Assist in providing access to technologies deemed essential for ICT security;	ASSIST CBM: assist in providing tech. deemed essential for ICT security
3:35	2014 - 2015 - UN GGE 2015 ICT re: International Security	2014	Create procedures for mutual assistance in responding to incidents and addressing short-term problems in securing networks, including procedures for expedited assistance;	EMERGENCY RESPONSE CBM: create procedures for mutual assistance in times of incident response
3:37	2014 - 2015 - UN GGE 2015 ICT re: International Security	2014	Facilitate cross-border cooperation to address critical infrastructure vulnerabilities that transcend national borders	PRODUCT CBM: transparency and dialogue regarding ICT vulnerabilities and identified harmful hidden functions in ICT products
3:38	2014 - 2015 - UN GGE 2015 ICT re: International Security	2014	Develop strategies for sustainability in ICT security capacity-building efforts;	CAPACITY BUILDING CBM: develop strategies for sustanability in ICT security (capacity-building)

ID	Document	Document Groups	Quotation Content	Codes
3:39	2014 - 2015 - UN GGE 2015 ICT re: International Security	2014	Prioritize ICT security awareness and capacity-building in national plans and budgets, and assign it appropriate weight in development and assistance planning.	CAPACITY BUILDING CBM: assign appropriate weight to ICT security awareness and capacity building in development and assistance planning CAPACITY BUILDING CBM: pioritize ICT security awareness and capacity-building in national plans and budgets
3:40	2014 - 2015 - UN GGE 2015 ICT re: International Security	2014	Encourage further work in capacity-building, such as on forensics or on cooperative measures to address the criminal or terrorist use of ICTs	CAPACITY BUILDING CBM: encourage further work in capacity-building
3:41	2014 - 2015 - UN GGE 2015 ICT re: International Security	2014	The development of regional approaches to capacity-building would be beneficial, as they could take into account specific cultural, geographic, political, economic or social aspects and allow a tailored approach	CAPACITY BUILDING CBM: develop regional approaches to capacity-building
3:44	2014 - 2015 - UN GGE 2015 ICT re: International Security	2014	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.	INTERNATIONAL LAW for: applicability of international law to cyberspace
3:46	2014 - 2015 - UN GGE 2015 ICT re: International Security	2014	respect for human rights and fundamental freedoms; and non-intervention in the internal affairs of other States	STATE SOVEREIGNTY for: state sovereignty applied to State's ICT activities & ICT infrastructure within their territory
3:51	2014 - 2015 - UN GGE 2015 ICT re: International Security	2014	The Group notes the established international legal principles, including, where applicable, the principles of humanity, necessity, proportionality and distinction;	CYBER ATTACKS disagreement: invoking countermeasures in response to cyber attacks
3:52	2014 - 2015 - UN GGE 2015 ICT re: International Security	2014	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;	CYBER ATTACKS against: using proxies for [international] wrongful cyber acts
3:53	2014 - 2015 - UN GGE 2015 ICT re: International Security	2014	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.	STATE SOVEREIGNTY disagreement: finding States at fault for internationally recognized wrongful ICT acts committed by on state territory
3:54	2014 - 2015 - UN GGE 2015 ICT re: International Security	2014	Further development by States collectively and individually of concepts for international peace and security in the use of ICTs at the legal, technical and policy levels	CONFIDENCE BUILDING for: further developement of concepts for international peace and security in the legal use of ICTs (technical and policy level)
3:55	2014 - 2015 - UN GGE 2015 ICT re: International Security	2014	Increased cooperation at regional and multilateral levels to foster common understandings on the potential risks to international peace and security posed by the malicious use of ICTs and on the security of ICT-enabled critical infrastructure.	CRITICAL INFRASTRUCTURE for: protecting critical infrastructures STAKEHOLDER COOPERATION CBM: form bilateral and multilateral cooperation initiatives to build on established partnerships/relationships
3:56	2014 - 2015 - UN GGE 2015 ICT re: International Security	2014	While States have a primary responsibility for maintaining a secure and peaceful ICT environment, effective international cooperation would benefit from identifying mechanisms for the participation, as appropriate, of the private sector, academia and civil society organization	STAKEHOLDER COOPERATION for: encourage participation of other stakeholders such as the private sector, academia, and civil society orgs (as appropriate) for CBM and/or norm creation and implementation
3:57	2014 - 2015 - UN GGE 2015 ICT re: International Security	2014	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	STATE RESPONSIBILITY for: dialogue amongst nations by an international body
4:2	2012 - 2013 - UN GGE ICT re: International Security	2012	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, peaceful and accessible ICT environment.	INTERNATIONAL LAW for: applicability of international law to cyberspace
4:3	2012 - 2013 - UN GGE ICT re: International Security	2012	State sovereignty and international norms and principles that flow from sovereignty apply to State conduct of ICT-related activities, and to their jurisdiction over ICT infrastructure within their territory	STATE SOVEREIGNTY for: state sovereignty applied to State's ICT activities & ICT infrastructure within their territory
4:4	2012 - 2013 - UN GGE ICT re: International Security	2012	State efforts to address the security of ICTs must go hand-in-hand with respect for human rights and fundamental freedoms set forth in the Universal Declaration of Human Rights and other international instruments	HUMAN RIGHTS for: respecting human rights and fundamental freedoms; applying them to cyber space / ICT use, etc.
4:5	2012 - 2013 - UN GGE ICT re: International Security	2012	States should intensify cooperation against criminal or terrorist use of ICTs, harmonize legal approaches as appropriate and strengthen practical collaboration between respective law enforcement and prosecutorial agencies	STAKEHOLDER COOPERATION for: work with states and/or the private sector/civil society (international and/or domestic) to further cooperate on topics such as law enforcement, prosecution, investment, e-commerce, intellectual property rights, etc.
4:6	2012 - 2013 - UN GGE ICT re: International Security	2012	States must meet their international obligations regarding internationally wrongful acts attributable to them.	STATE RESPONSIBILITY for: states must meet international obligations regarding internationally wrongful acts attributed to them
4:7	2012 - 2013 - UN GGE ICT re: International Security	2012	States must not use proxies to commit internationally wrongful acts	CYBER ATTACKS against: using proxies for [international] wrongful cyber acts

ID	Document	Document Groups	Quotation Content	Codes
4:8	2012 - 2013 - UN GGE ICT re: International Security	2012	States should seek to ensure that their territories are not used by non-State actors for unlawful use of ICTs.	STATE RESPONSIBILITY & SOVEREIGNTY against: allowing non-State actors in their territories to unlawfully use ICT
4:10	2012 - 2013 - UN GGE ICT re: International Security	2012	The exchange of views and information on a voluntary basis on national strategies and policies, best practices, decision-making processes, relevant national organizations and measures to improve international cooperation.	INFORMATION EXCHANGE CBM: encouraging exchanges between research and academic institutions INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information
4:11	2012 - 2013 - UN GGE ICT re: International Security	2012	The creation of bilateral, regional and multilateral consultative frameworks for confidence-building, which could entail workshops, seminars and exercises to refine national deliberations on how to prevent disruptive incidents arising from State use of ICTs and how these incidents might develop and be managed	STAKEHOLDER COOPERATION CBM: form bilateral and multilateral cooperation initiatives to build on established partnerships/relationships
4:13	2012 - 2013 - UN GGE ICT re: International Security	2012	Exchanges of information and communication between national Computer Emergency Response Teams (CERTs) bilaterally, within CERT communities, and in other forums, to support dialogue at political and policy levels	STAKEHOLDER COOPERATION CBM: states should support/facilitate cooperation amongst national response teams and other relevant entities
4:14	2012 - 2013 - UN GGE ICT re: International Security	2012	Increased cooperation to address incidents that could affect ICT or critical infrastructure that rely upon ICT-enabled industrial control systems. This could include guidelines and best practices among States against disruptions perpetrated by non-State actors;	CONFIDENCE BUILDING CBM: address issues [related to cyber space/cybersecurity/ICTs] INFORMATION EXCHANGE AND TRANSPARENCY for: cooperate/exchange guidelines and/or best practices against disruptions by non-State actors
4:16	2012 - 2013 - UN GGE ICT re: International Security	2012	Enhanced mechanisms for law enforcement cooperation to reduce incidents that could otherwise be misinterpreted as hostile State actions would improve international security	STAKEHOLDER COOPERATION CBM: enhance law enforcement cooperation to reduce incidents that may be misinterpreted as hostile State actions
4:18	2012 - 2013 - UN GGE ICT re: International Security	2012	While States must lead in the development of confidence-building measures, their work would benefit from the appropriate involvement of the private sector and civil society	STAKEHOLDER COOPERATION for: encourage participation of other stakeholders such as the private sector, academia, and civil society orgs (as appropriate) for CBM and/or norm creation and implementation
4:19	2012 - 2013 - UN GGE ICT re: International Security	2012	Given the pace of ICT development and the scope of the threat, the Group believes there is a need to enhance common understandings and intensify practical cooperation. In this regard, the Group recommends regular institutional dialogue with broad participation under the auspices of the United Nations, as well as regular dialogue through bilateral, regional and multilateral forums, and other international organizations.	STATE RESPONSIBILITY for: dialogue amongst nations by an international body
4:20	2012 - 2013 - UN GGE ICT re: International Security	2012	improve the security of critical ICT infrastructure; develop technical skill and appropriate legislation, strategies and regulatory frameworks to fulfil their responsibilities; and bridge the divide in the security of ICTs and their use	CRITICAL INFRASTRUCTURE CBM: improve security of critical ICT infrastructure
4:21	2012 - 2013 - UN GGE ICT re: International Security	2012	In this regard, States working with international organizations, including United Nations agencies and the private sector, should consider how best to provide technical and other assistance to build capacities in ICT security and their use in countries requiring assistance, particularly developing countries	CAPACITY BUILDING CBM: encourage further work in capacity-building
4:22	2012 - 2013 - UN GGE ICT re: International Security	2012	Supporting bilateral, regional, multilateral and international capacity-building efforts to secure ICT use and ICT infrastructures; to strengthen national legal frameworks, law enforcement capabilities and strategies; to combat the use of ICTs for criminal and terrorist purposes; and to assist in the identification and dissemination of best practices	CAPACITY BUILDING CBM: encourage further work in capacity-building STAKEHOLDER COOPERATION for: work / intensify cooperation against criminal/terrorist use of ICTs
4:23	2012 - 2013 - UN GGE ICT re: International Security	2012	Creating and strengthening incident response capabilities, including CERTs, and strengthening CERT-to-CERT cooperation	EMERGENCY RESPONSE CBM: each state/regional partnership should establish and/or strengthen a national computer emergency response team (CERT) / cybersecurity incident response team
4:24	2012 - 2013 - UN GGE ICT re: International Security	2012	Supporting the development and use of e-learning, training and awareness-raising with respect to ICT security to help overcome the digital divide and to assist developing countries in keeping abreast of international policy developments;	ASSISTANCE CBM: provide assistance and training to developing countries to improve cybsecurity and ICT use
4:25	2012 - 2013 - UN GGE ICT re: International Security	2012	Increasing cooperation and transfer of knowledge and technology for managing ICT security incidents, especially for developing countries	ASSISTANCE CBM: provide assistance and training to developing countries to improve cybsecurity and ICT use
4:27	2012 - 2013 - UN GGE ICT re: International Security	2012	Encouraging further analysis and study by research institutes and universities on matters related to ICT security	INFORMATION EXCHANGE CBM: encourage further analysis and study by research institutes and universities on ICT security related matters

ID	Document	Document Groups	Quotation Content	Codes
4:28	2012 - 2013 - UN GGE ICT re: International Security	2012	Building cooperation for a peaceful, secure, resilient and open ICT environment	CRITICAL INFRASTRUCTURE for: promoting resilience (as related to ICTs,cybersecurity, and related critical infrastructure DIGITAL ECONOMY for: promote resilience of financial services and institutions against malicious use of ICTs
4:29	2012 - 2013 - UN GGE ICT re: International Security	2012	4. Numerous bilateral, regional and multilateral initiatives since 2010 highlight the growing importance accorded to greater security of and in the use of ICTs, reducing risks to public safety, improving the security of nations and enhancing global stability. It is in the interest of all States to promote the use of ICTs for peaceful purposes. States also have an interest in preventing conflict arising from the use of ICTs. Common understandings on norms, rules and principles applicable to the use of ICTs by States and voluntary confidence-building measures can play an important role in advancing peace and security. Although the work of the international community to address this challenge to international peace and security is at an early stage, a number of measures concerning norms, rules and principles for responsible State behaviour can be identified for further consideration.	STAKEHOLDER COOPERATION CBM: form bilateral and multilateral cooperation initiatives to build on established partnerships/relationships STAKEHOLDER COOPERATION CBM: states should participate and cooperate in multilateral forums
4:30	2012 - 2013 - UN GGE ICT re: International Security	2012	2. International cooperation is essential to reduce risk and enhance security. For this reason, the General Assembly requested the Secretary-General, with the assistance of a group of governmental experts, to continue to study possible cooperative measures to address existing and potential threats (resolution 66/24), and submit a report to the sixty-eighth session of the Assembly. The present report builds upon the 2010 report (A/65/201) from the previous Group of Governmental Experts, which examined this topic and made recommendations for future work. 3. The 2010 report recommended further dialogue among States on n	STATE RESPONSIBILITY for: adhering to rules and regulations agreed upon by previously enacted international law/mandates/treaties
5:2	2019 - GCSC Final Report	2019	protect electoral systems	CYBER STABILITY for: protecting political systems
5:3	2019 - GCSC Final Report	2019	GCSC believes that responsibilities should be imposed on non-state actors as well, as they must exercise restraint or take afrmative steps to ensure the stability of cyberspace	NON-STATE RESPONSIBILITY for: responsibilities should be imposed on non-state actos as well (regarding lawful use of ICTs, cybersecurity, maintaining stability and international security/peace, etc.)
5:4	2019 - GCSC Final Report	2019	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.	CYBER STABILITY for: protecting the public core of the internet
5:5	2019 - GCSC Final Report	2019	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	CYBER ATTACKS against: conducting ICT operations intended to disrupt essential infrastructure of political processes (i.e., election processes)
5:6	2019 - GCSC Final Report	2019	State and non-state actors should not tam- per with products and services in develop- ment and production, nor allow them to be tampered with, if doing so may substantially impair the stability of cyberspace	PRODUCT TAMPERING against: states and non-state actors tampering with products/services (knowingly inserting harmful material into their products) NOR allowing their products to be tampered with
5:7	2019 - GCSC Final Report	2019	State and non-state actors should not com- mandeer the general public's ICT resources for use as botnets or for similar purposes.	CYBER ATTACKS against: comandeering the general public's ICT resources for use as botnets or for similar purposes
5:8	2019 - GCSC Final Report	2019	States should create procedurally transparent frameworks to assess whether and when to disclose not publicly known vulnerabilities or faws they are aware of in information sys- tems and technologies. The default presump- tion should be in favor of disclosure	PRODUCT for: creating transparent procedures and frameworks to asses whether and when to disclose not publicly known vulnerabilities or flaws in their information systems and/or technologies
5:9	2019 - GCSC Final Report	2019	y and GLOBAL COMMISSION 22 GLOBAL COMMISSION ON THE STABILITY OF CYBERSPACE ON THE STABILITY OF CYBERSPACE stability	PRODUCT for: developers and producers of products and services should prioritize security and stability
5:10	2019 - GCSC Final Report	2019	take reasonable steps to ensure that their products or services are free from signifcant vulnerabilities,	PRODUCT for: developers and producers of products and services should take reasonable steps to ensure that their products/services are free from significant vulnerabilities
5:11	2019 - GCSC Final Report	2019	take mea- sures to timely mitigate vulnerabilities that are later discovered and to be transparent about their process	PRODUCT for: developers and producers of products and services should take measures to timely mitigate vulnerabilities that are later discovered and be transparent about their process
5:12	2019 - GCSC Final Report	2019	States should enact appropriate measures, including laws and regulations, to ensure basic cyber hygiene	STATE RESPONSIBILITY for: nation-state enacted laws and/or regulations to ensure basic cyber protocols/cleanliness/hygiene

ID	Document	Document Groups	Quotation Content	Codes
5:13	2019 - GCSC Final Report	2019	Non-state actors should not engage in ofen- sive cyber operations and state actors should prevent such activities and respond if they occur.	INFORMATION EXCHANGE AND TRANSPARENCY for: cooperate/exchange guidelines and/or best practices against disruptions by non-State actors STATE RESPONSIBILITY & SOVEREIGNTY against: allowing non-State actors in their territories to unlawfully use ICT
5:14	2019 - GCSC Final Report	2019	Second, there needs to be greater awareness of proposed norms by the entities that are capable of their implementation, as well as those the norms are meant to protect	NORMS for: promote awareness of existing and/or proposed norms, as well as support their operationalization
5:17	2019 - GCSC Final Report	2019	State and non-state actors must adopt and implement norms that increase the stability of cyberspace by promoting restraint and encouraging action	CYBERSPACE STABILITY for: both nation states and non-state actors must adopt and implement norms that increase the stabilitiy of cyberspace (promoting restraint and encouraging action)
5:18	2019 - GCSC Final Report	2019	State and non-state actors, consistent with their responsibilities and limitations, must respond appropriately to norms violations, ensuring that those who violate norms face predictable and meaningful consequences	STATE RESPONSIBILITY & SOVEREIGNTY for: nation states and non-state actors (consistent with their responsibilities and limitations) must respond appropriately to norms violations, ensuring that those who violate norms face predictable and meaningful consequences
5:19	2019 - GCSC Final Report	2019	State and non-state actors, including international institutions, should increase eforts to train staf, build capacity and capabilities, promote a shared understanding of the importance of the stability of cyberspace, and take into account the disparate needs of diferent parties.	CYBERSPACE STABILITY for: state and non-state actors (including international entities) should increase efforts to build capacity and capabilities (i.e., train staff) and promote a shared understanding of the importance of the stability of cyberspace
5:20	2019 - GCSC Final Report	2019	State and non-state actors should collect, share, review, and publish information on norms violations and the impact of such activities	INFORMATION EXCHANGE AND TRANSPARENCY for: states and non-state actors should collect, share, review, and publish information on norms violations and the impact of such activities
5:21	2019 - GCSC Final Report	2019	State and non-state actors should establish and support Communities of Interest to help ensure the stability of cyberspace.	CYBERSPACE STABILITY for: state and non-state actors should estsablish and support Communities of Interest to help ensure the stability of cyberspace
5:22	2019 - GCSC Final Report	2019	The GCSC recommends establishing a standing multistakeholder engagement mechanism to address stability issues, one where states, the private sector (including the technical community), and civil society are adequately involved and consulted.	STAKEHOLDER COOPERATION for: establishing a standing multistakeholder engagement mechanism in order to address stability issues (this includes adequate involvement and consultation of states, non-state actors such as private sector entities, and civil society)
6:1	2009 - 2010 - UN GGE	2009	Confidence-building, stability and risk reduction measures to address the implications of State use of ICTs, including exchanges of national views on the use of ICTs in conflict	INFORMATION EXCHANGE CBM: exchange national views on the use of ICTS in conflicts
6:2	2009 - 2010 - UN GGE	2009	Further dialogue among States to discuss norms pertaining to State use of ICTs, to reduce collective risk and protect critical national and international infrastructure;	NORMS CBM: further dialogue regarding norms pertaining to State use of ICTs
6:3	2009 - 2010 - UN GGE	2009	Information exchanges on national legislation and national information and communications technologies security strategies and technologies, policies and best practices;	INFORMATION EXCHANGE AND TRANSPARENCY for: cooperate/exchange guidelines and/or best practices against disruptions by non-State actors INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information
6:4	2009 - 2010 - UN GGE	2009	Identification of measures to support capacity-building in less developed countries	ASSISTANCE CBM: provide assistance and training to developing countries to improve cybsecurity and ICT use
7:3	2020 - UN OWEG (2nd pre-draft)	2020	States reiterated that voluntary, non-binding norms of responsible State behaviour are consistent with international law and with the purposes and principles of the United Nations, including to maintain international peace and security and the promotion of human rights.	CONFIDENCE BUILDING CBM: promote the use of ICTs for peaceful purposes HUMAN RIGHTS for: respecting human rights and fundamental freedoms; applying them to cyber space / ICT use, etc. INTERNATIONAL LAW for: applicability of international law to cyberspace
7:4	2020 - UN OWEG (2nd pre-draft)	2020	States highlighted that norms should not place undue restrictions on international cooperation and technology transfer, nor hinder innovation for peaceful purposes and the economic development of States	NORMS rule: norms should not place undue restrictions on international cooperation/tech. transfer, nor should they hinder innovation for peaceful purposes and the economic development of states

ID	Document	Document Groups	Quotation Content	Codes
7:6	2020 - UN OWEG (2nd pre-draft)	2020	States stressed the need to promote awareness of the existing norms and support their operationalization. While these norms articulate what actions States should or should not take, States underscored the need for guidance on how to operationalize them. In this regard, States called for the sharing and dissemination of good practices and lessons on norm implementation. 6 A/70/174, paragraph 13. 7 A/69/723. 8 Different cooperative approaches were also proposed, such as developing a roadmap to assist States in their implementation efforts and surveys for the sharing of good practices.	INFORMATION EXCHANGE CBM: develop a roadmap to assist States in their implementation efforts and surveys for the sharing of good practices (re: CBM and/or norm implementation) NORMS for: promote awareness of existing and/or proposed norms, as well as support their operationalization NORMS for: sharing and dissemination of good practices and lessons on norm impementation
7:7	2020 - UN OWEG (2nd pre-draft)	2020	enhancement as well as further elaboration of norms	NORMS proposal: enhance and further elaborate of norms
7:8	2020 - UN OWEG (2nd pre-draft)	2020	Such proposals included, inter alia, that States affirm their commitment to a culture of restraint and to international peace and security in their use of ICTs	CONFIDENCE BUILDING for: further developement of concepts for international peace and security in the legal use of ICTs (technical and policy level)
7:9	2020 - UN OWEG (2nd pre-draft)	2020	reaffirm their primary responsibility for maintaining a secure, safe and trustable ICT environment	CYBER STABILITY for: maintaining a secure, safe, and trustable ICT environment
7:10	2020 - UN OWEG (2nd pre-draft)	2020	general availability or integrity of the public core of the Internet should be protected	CYBER STABILITY for: protecting the public core of the internet
7:11	2020 - UN OWEG (2nd pre-draft)	2020	States should not conduct ICT operations intended to disrupt the infrastructure essential to political processes or to harm medical facilities.	CRITICAL INFRASTRUCTURE against: knowingly damaging critical infrastructure
7:12	2020 - UN OWEG (2nd pre-draft)	2020	States should not conduct ICT operations intended to disrupt the infrastructure essential to political processes or to harm medical facilities	CYBER ATTACKS against: conducting ICT operations intended to disrupt essential infrastructure of medical facilities CYBER ATTACKS against: conducting ICT operations intended to disrupt essential infrastructure of political processes (i.e., election processes)
7:13	2020 - UN OWEG (2nd pre-draft)	2020	States also proposed further ensuring the integrity of the ICT supply chain, expressing concern over the creation of harmful hidden functions in ICT products,	DIGITAL ECONOMY for: further ensuring the integrity of the ICT supply chain
7:14	2020 - UN OWEG (2nd pre-draft)	2020	the responsibility to notify users when significant vulnerabilities are identified.	DIGITAL ECONOMY for: states are responsible to notify ICT supply chain/product users when significant vulnerabilities are identified
7:15	2020 - UN OWEG (2nd pre-draft)	2020	protection of transborder critical information infrastructure, as a distinct category of critical infrastructure, is the shared responsibility of all States.	STATE RESPONSIBILITY for: protecting transborder critical information infrastructure is a shared responsibility of all States
7:18	2020 - UN OWEG (2nd pre-draft)	2020	States could be called on to take the necessary outreach, cooperation and, where necessary, regulatory steps to ensure that various stakeholders, including the public and private sectors and civil society, uphold their responsibilities.	STATE RESPONSIBILITY/SOVEREIGNTY for: States could be called on to take the necessary outreach, cooperation, and where necessary, regulatory steps to ensure that various stakeholders uphold their responsibilities
7:20	2020 - UN OWEG (2nd pre-draft)	2020	In their discussions at the OEWG, States reaffirmed the value of CBMs in increasing transparency, predictability and stability.	CONFIDENCE BUILDING CBM: CBM are important for increasing transparency, predictability, and stability
7:21	2020 - UN OWEG (2nd pre-draft)	2020	need to translate confidence-building measures into concrete actions that are implementable by all States.	CONFIDENCE BUILDING CBM: translate CBMs into concrete actions that are implementable by all states
7:22	2020 - UN OWEG (2nd pre-draft)	2020	regular dialogue and voluntary 9 information exchanges on existing and emerging threats, national policy or doctrine, national views on how international law applies to State use of ICTs, and national approaches to defining critical infrastructure or categorizing ICT-related incidents	CONFIDENCE BUILDING CBM: classification/categorization of ICT incidents CONFIDENCE BUILDING CBM: voluntary transparency CRITICAL INFRASTRUCTURE CBM: define critical infrastructure INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information
7:24	2020 - UN OWEG (2nd pre-draft)	2020	training for diplomats,	CONFIDENCE BUILDING CBM: develop guidance on training diplomats
7:25	2020 - UN OWEG (2nd pre-draft)	2020	exchanging lessons on establishing and exercising secure crisis communication channels,	EMERGENCY RESPONSE CBM: develop guidance in order to exchange lessons on establishing and exercising secure crisis communication channels
7:26	2020 - UN OWEG (2nd pre-draft)	2020	scenario-based exercises at the policy level as well as operational exercises at the technical level between Computer Emergency Response Teams (CERTs) or Computer Security Incident Response Teams (CSIRTs).	EMERGENCY RESPONSE CBM: develop guidance on scenario-based exercises at the policy, operational, and technical level between nation states and their Computer Emergency Response Teams (CERTs) and/or Computer Security Incident Response Teams (CSIRTs)

ID	Document	Document Groups	Quotation Content	Codes
7:27	2020 - UN OWEG (2nd pre-draft)	2020	It was noted that national declarations of adherence to the normative framework of responsible State behaviour could build trust and confidence between States.	NORMS CBM: national declarations of adherence to the normative framework of responsible State behavior could build trust and confidence between states
7:28	2020 - UN OWEG (2nd pre-draft)	2020	States stressed that establishing national Points of Contact (PoCs) is a CBM in itself, but is also a prerequisite for the implementation of many other CBMs, and is invaluable in times of crisis. States may find it useful to have PoCs for, inter alia, diplomatic, policy, legal and technical exchanges, as well as incident reporting and response	CONFIDENCE BUILDING CBM: establishing national/international/regional/sub-regional Points of Contact (POCs) is a CBM as well as a prerequisite for the implementation of many other CBMs (i.e., useful for diplomatic, policy, legal and technical exchanges, as well as incident reporting and responses)
7:29	2020 - UN OWEG (2nd pre-draft)	2020	It was suggested that a global directory of Points of Contact would be useful and could take into account the experiences from regional bodies in this area. At the same time, it was noted that the security of such a directory as well as its operational modalities would be crucial to its effectiveness.	CONFIDENCE BUILDING CBM: a global directory of Points of Contact (POCs) would be useful
7:30	2020 - UN OWEG (2nd pre-draft)	2020	The value of regularly conducting exercises among a network of PoCs was also emphasized, as it can help to maintain readiness as well as responsiveness and ensure that PoC directories remain updated.	EMERGENCY RESPONSE CBM: regularly conducting exercises among a network of Point of Contacts (POCs) could be valuable
7:31	2020 - UN OWEG (2nd pre-draft)	2020	States proposed the establishment of a global repository of CBMs, with the objective of sharing policy, good practice, experiences and assessments with CBM implementation and encouraging peer learning. Such a repository could also assist States to identify additional CBMs appropriate to their national and regional contexts.	CONFIDENCE BUILDING CBM: establish a global repository of CBMs with the objective of sharing policy, good/best practices, experiences, and assessments of CBM implementation as well as encouraging peer learning
7:32	2020 - UN OWEG (2nd pre-draft)	2020	States emphasized 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.	EMERGENCY RESPONSE CBM: each state/regional partnership should establish and/or strengthen a national computer emergency response team (CERT) / cybersecurity incident response team
7:33	2020 - UN OWEG (2nd pre-draft)	2020	it is important that other fora be used to promote CBMs as well.	STAKEHOLDER COOPERATION CBM: it is important for other stakeholders such as regional and sub-regional bodies/entities be used to create, promote, and implement CBMs
7:34	2020 - UN OWEG (2nd pre-draft)	2020	States also proposed that some CBMs developed at the regional level could serve as useful models for adaptation in wider contexts.	CAPACITY BUILDING CBM: some CBMs developed at the regional level could serve as useful models for adaptation in wider contexts
7:35	2020 - UN OWEG (2nd pre-draft)	2020	States drew attention to the roles and responsibilities of other actors, including the private sector, academia and civil society, in contributing to building trust and confidence in the use of ICTs at national, regional and global levels. States noted the variety of multi-stakeholder initiatives that, through the development of principles and commitments, have established new networks for exchange, collaboration and cooperation. In a similar vein, sector- or domain-specific initiatives have demonstrated the growing awareness of the roles and responsibilities of other actors and 10 the unique contributions that they can make to ICT security through voluntary commitments, professional codes and standards	STAKEHOLDER COOPERATION for: encourage participation of other stakeholders such as the private sector, academia, and civil society orgs (as appropriate) for CBM and/or norm creation and implementation
8:1	2020 - Singapore/Australia Renewed MOU on Cybersecurity Cooperation	2020	information exchange and sharing	INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information
8:2	2020 - Singapore/Australia Renewed MOU on Cybersecurity Cooperation	2020	joint cybersecurity exercises	STAKEHOLDER COOPERATION for: conduct joint cybersecurity and/or related law enforcement exercises between nation states
8:3	2020 - Singapore/Australia Renewed MOU on Cybersecurity Cooperation	2020	training to develop awareness and skills	NORM for: promote cooperation in training to develop ICT/cybersecurity awareness and skills
8:4	2020 - Singapore/Australia Renewed MOU on Cybersecurity Cooperation	2020	sharing of best practices and promoting innovation	INFORMATION EXCHANGE for: sharing of good/best practices in relation to ICTs and cybersecurity
8:5	2020 - Singapore/Australia Renewed MOU on Cybersecurity Cooperation	2020	regional confidence-building measures	CONFIDENCE BUILDING for: promote cooperation in regional confidence-building measures (CBMs)
8:6	2020 - Singapore/Australia Renewed MOU on Cybersecurity Cooperation	2020	regional capacity building	CAPACITY BUILDING CBM: develop regional approaches to capacity-building

ID	Document	Document Groups	Quotation Content	Codes
9:1	2020 - EU/US cybersecurity project	2020	Continue to share information on insurer cybersecurity and operational resilience including, for example, discussing insurance industry approaches to managing cybersecurity risk	INFORMATION EXCHANGE for: sharing information related to insurance industry cybersecurity
9:2	2020 - EU/US cybersecurity project	2020	supervisory approaches to reviewing insurers' cybersecurity measures	DIGITAL ECONOMY for: supervisory approaches to reviewing insurers' cybersecurity measures (insurance cybersecurity)
9:3	2020 - EU/US cybersecurity project	2020	preventing and managing a cross-border cyber event from both a supervisory and industry perspective	EMERGENCY RESPONSE for: prevent and manage a cross-border (international/transnational) cyber event from both supervisory and industry perspective
9:4	2020 - EU/US cybersecurity project	2020	cybersecurity implications of insurers' increased outsourcing to the cloud	TRANSPARENCY for: continuing to share information on the cybersecurity implications of insurers' increased outsourcing to the cloud
9:5	2020 - EU/US cybersecurity project	2020	Complete development of an initial cybersecurity exercise template for EU and US supervisors on how to coordinate a cross-border response in the event of an international cybersecurity incident.	EMERGENCY RESPONSE CBM: develop guidance on scenario-based exercises at the policy, operational, and technical level between nation states and their Computer Emergency Response Teams (CERTs) and/or Computer Security Incident Response Teams (CSIRTs)
10:1	2020 - Japan/Estonia Summit Meeting	2020	regular exchanges of information and consultations between our authorities	INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information
11:1	2020 - U.S./Canada Cyber Relations	2020	These efforts include collaboration along four lines of effort: addressing threats early; facilitating lawful trade and travel; enhancing law enforcement collaboration; and promoting resilience, including of critical infrastructure and cybersecurity.	CRITICAL INFRASTRUCTURE for: promoting resilience (as related to ICTs,cybersecurity, and related critical infrastructure CRITICAL INFRASTRUCTURE for: protecting critical infrastructures INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information
12:1	2019 - ASEAN/U.S. Cyber Policy Dialogue	2019	including its recommendations to enhance trust, confidence and cooperation	CONFIDENCE BUILDING for: enhance trust,, confidence, and cooperation regarding ICTs, cyberspace and cybersecurity
12:2	2019 - ASEAN/U.S. Cyber Policy Dialogue	2019	promote an open, secure, stable, accessible and peaceful ICT environment,	NORM for: promote an open, secure, stable, accessible, and peaceful cyber space / ICT environment
12:3	2019 - ASEAN/U.S. Cyber Policy Dialogue	2019	call for all States to be guided in their use of ICTs by the 2015 Report of the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UNGGE)	UNITED NATIONS for: following the United Nation's (UN) [2015 and or 2013] GGE report's call for all States to be guided in their use of ICTs in relation to the report
13:1	2019 - Australia/Japan Cyber Policy Dialogue Joint Statement	2019	Australia and Japan reaffirmed their commitment to continue to enhance cooperation and information sharing on responses to malicious cyber activities, including deterring and responding to significant cyber incidents, consistent with relevant domestic and international law.	CYBER ATTACKS for: responding to requests for help in the event of a cyber attack CYBER STABILITY for: deterring cyber incidents / attacks DOMESTIC LAW for: applicability of domestic law to cyber space / ICT usage INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information INTERNATIONAL LAW for: applicability of international law to cyberspace
13:2	2019 - Australia/Japan Cyber Policy Dialogue Joint Statement	2019	adherence to agreed voluntary norms of responsible state behaviour during peacetime	STATE RESPONSIBILITY for: states should behave responsibly in cyberspace (and use ICTs responsibly) during peacetime
13:3	2019 - Australia/Japan Cyber Policy Dialogue Joint Statement	2019	development and implementation of practical cyber confidence building measures between states	CONFIDENCE BUILDING for: develop and implement [practical] cyber confidence building measures (CBMs) between nation states
13:4	2019 - Australia/Japan Cyber Policy Dialogue Joint Statement	2019	supported by coordinated capacity building programs. In this regard, Japan and Australia reaffirmed their commitment to work collaboratively on cyber capacity building across the region	CYBERSPACE STABILITY for: state and non-state actors (including international entities) should increase efforts to build capacity and capabilities (i.e., train staff) and promote a shared understanding of the importance of the stability of cyberspace
13:5	2019 - Australia/Japan Cyber Policy Dialogue Joint Statement	2019	Australia and Japan also reaffirmed their commitment to cooperate further on supply chain and IoT security.	DIGITAL ECONOMY for: further ensuring the integrity of the ICT supply chain

ID	Document	Document Groups	Quotation Content	Codes
13:6	2019 - Australia/Japan Cyber Policy Dialogue Joint Statement	2019	Australia and Japan reaffirmed their commitment to cooperate in multilateral forums on the further elaboration of international law and norms, confidence building measures and capacity building measures. This includes discussions in the United Nations, the G20, and the ASEAN Regional Forum Inter-Sessional Meeting on Security of and in the Use of Information and Communication Technologies (ARF-ISM on ICTs Security).	STAKEHOLDER COOPERATION CBM: states should participate and cooperate in multilateral forums
14:1	2014 - US/Japan Second Cyber Dialogue	2014	including critical infrastructure protection	CRITICAL INFRASTRUCTURE for: protecting critical infrastructures
14:2	2014 - US/Japan Second Cyber Dialogue	2014	wide-ranging bilateral cooperation on cyber issues,	CONFIDENCE BUILDING for: enhance trust,, confidence, and cooperation regarding ICTs, cyberspace and cybersecurity INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information
15:1	2019 - Singapore/Republic of Korea sign MOU to enhance cybersecurity cooperation	2019	enhancing cybersecurity cooperation	CONFIDENCE BUILDING for: enhance trust,, confidence, and cooperation regarding ICTs, cyberspace and cybersecurity
15:2	2019 - Singapore/Republic of Korea sign MOU to enhance cybersecurity cooperation	2019	This MOU will facilitate more exchanges and information-sharing across the strategic, policy, and technical domains	INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information
15:3	2019 - Singapore/Republic of Korea sign MOU to enhance cybersecurity cooperation	2019	protection of critical information infrastructure,	CRITICAL INFRASTRUCTURE for: protecting critical infrastructures
15:4	2019 - Singapore/Republic of Korea sign MOU to enhance cybersecurity cooperation	2019	promotion of the cybersecurity ecosystem	CONFIDENCE BUILDING for: promote the cybersecurity ecosystem
15:5	2019 - Singapore/Republic of Korea sign MOU to enhance cybersecurity cooperation	2019	human resource development,	CONFIDENCE BUILDING for: promote human resource development (as related to cyber space, ICTs, cybersecurity, etc.)
16:1	2019 - 11th BRICS Summit – Brasília Declaration	2019	continue to strengthen joint activities among BRICS countries, create new cooperation opportunities and expand and intensify partnerships already in progress including taking necessary steps for early setting up of the Digital BRICS Task Force (DBTF).	INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information STAKEHOLDER COOPERATION CBM: form bilateral and multilateral cooperation initiatives to build on established partnerships/relationships STAKEHOLDER COOPERATION for: conduct joint cybersecurity and/or related law enforcement exercises between nation states
16:2	2019 - 11th BRICS Summit – Brasília Declaration	2019	their eàorts to further our cooperation on topics such as investment, e-commerce, micro, small and medium enterprises (MSMEs) and intellectual property rights in cooperation with specialized BRICS IP OÞces.	STAKEHOLDER COOPERATION for: work with states and/or the private sector/civil society (international and/or domestic) to further cooperate on topics such as law enforcement, prosecution, investment, e-commerce, intellectual property rights, etc.
16:3	2019 - 11th BRICS Summit – Brasília Declaration	2019	call for enhanced intra-BRICS cooperation at relevant multilateral fora, including in trade facilitation, law enforcement, use of advanced information technologies and capacity building.	CYBERSPACE STABILITY for: state and non-state actors (including international entities) should increase efforts to build capacity and capabilities (i.e., train staff) and promote a shared understanding of the importance of the stability of cyberspace
16:4	2019 - 11th BRICS Summit – Brasília Declaration	2019	including in digital infrastructure, skills development, particularly for young people, sustainable investment, investment in local basic services, and outward investment to areas of high potential growth, including on the African continent.	EDUCATION CBM: skills development, particularly for younger individuals (both internal and external, international and/or domestic)
16:5	2019 - 11th BRICS Summit – Brasília Declaration	2019	we underscore the importance of BRICS cooperation in agriculture. We recognize the importance of science-based agriculture and of deploying ICT to that end. We underline the need of ensuring food security, food safety, addressing malnutrition, eliminating hunger and poverty through increased agricultural production, productivity, sustainable management of natural resources and trade in agriculture among the BRICS countries	FOOD SECURITY for: utilizing ICTs in order to ensure food security, food safety, addressing malnutrition, and working towards eliminating hunger and poverty (via agricultural production, productivity, sustainability, management of natural resources, and trade)
16:6	2019 - 11th BRICS Summit – Brasília Declaration	2019	We underscore the importance of an open, secure, peaceful, stable, accessible and non-discriminatory environment for information and communications technologies (ICTs).	CYBER STABILITY for: maintaining a secure, safe, and trustable ICT environment NORM for: promote an open, secure, stable, accessible, and peaceful cyber space / ICT environment

ID	Document	Document Groups	Quotation Content	Codes
16:7	2019 - 11th BRICS Summit – Brasília Declaration	2019	We emphasize the importance of universally agreed norms, rules and principles,	CYBERSPACE STABILITY for: both nation states and non-state actors must adopt and implement norms that increase the stabilitiy of cyberspace (promoting restraint and encouraging action)
16:8	2019 - 11th BRICS Summit – Brasília Declaration	2019	We emphasize the importance of universally agreed norms, rules and principles, under the auspices of the UN, for the responsible behavior of States in the realm of ICTs	NORMS CBM: universally agreed upon [voluntary] norms/rules/principles are important for the responsible behavior of States' use of ICTs UNITED NATIONS CBM: the United Nations (UN) may serve as an international body for decision-making, framework creation/implementation, and when developing and adopting universally agreed upon ICT norms/rules/principles (in order to ensure peace and responsible behavior/ICT use)
16:9	2019 - 11th BRICS Summit – Brasília Declaration	2019	We reaÞrm our commitment to tackling the misuse of ICTs for criminal and terrorist activities	STAKEHOLDER COOPERATION for: work / intensify cooperation against criminal/terrorist use of ICTs
16:11	2019 - 11th BRICS Summit – Brasília Declaration	2019	Bearing in mind previous BRICS Summits, we reaÞrm the importance of establishing legal frameworks of cooperation among BRICS member States on ensuring security in the use of ICTs and acknowledge the work of the WGSICT towards consideration and elaboration of proposals on this matter.	CAPACITY BUILDING CBM: develop regional approaches to capacity-building CONFIDENCE BUILDING for: promote cooperation in regional confidence-building measures (CBMs)
17:1	2019 - China/Germany dialogue tackles security threats	2019	The discussions focused on counter-terrorism and fighting transnational organized crimes involving cyber security and economy, and the two sides reached a consensus on what practical actions to take. They also agreed on areas for further cooperation	INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information
17:2	2019 - China/Germany dialogue tackles security threats	2019	Li also said that the two counties also face other mutual security threats, such as organized crime and cyber crimes. Those threats don't exist independently, and not a single country can fight those crimes alone, said Li. He said that security cooperation appears to be more urgent as economic cooperation between China and Germany deepens.	STAKEHOLDER COOPERATION CBM: form bilateral and multilateral cooperation initiatives to build on established partnerships/relationships
17:3	2019 - China/Germany dialogue tackles security threats	2019	He said that security cooperation appears to be more urgent as economic cooperation between China and Germany deepens. "Economic cooperation is hard to maintain if it faces various security threats, so jointly cracking down on those threats sustains the two countries' economic ties," said Li	STAKEHOLDER COOPERATION CBM: cooperation between states/entities (domestic and/or international) is important for furthering economic relationships/development
18:1	2019 - U.S./EU Cyber Dialogue : Joint Elements Statement on the Sixth Summit	2019	The United States and the European Union reaffirmed their commitment to a global, open, stable and secure cyberspace where the rule of law is fully respected, where the same rights that individuals have offline are also protected online, and where the security, economic growth, prosperity, and integrity of free and democratic societies is promoted and preserved	CYBER STABILITY for: maintaining a secure, safe, and trustable ICT environment HUMAN RIGHTS for: respecting human rights and fundamental freedoms; applying them to cyber space / ICT use, etc.
18:2	2019 - U.S./EU Cyber Dialogue : Joint Elements Statement on the Sixth Summit	2019	The discussions addressed coordination and cooperation toward bolstering cyber resilience, combatting cybercrime, preserving multi-stakeholder Internet governance, ensuring international cyber stability and security, furthering cyber diplomacy and deterrence, and building cyber capacity. Both sides welcomed continued progress on increasing global capabilities to better prevent, protect against, detect, deter, and respond to malicious cyber activities and underlined the need for coordination and cooperation in order to safeguard a global, open, stable, and secure cyberspace.	CAPACITY BUILDING CBM: encourage further work in capacity-building CRITICAL INFRASTRUCTURE for: promoting resilience (as related to ICTs,cybersecurity, and related critical infrastructure CYBER STABILITY for: deterring cyber incidents / attacks CYBER STABILITY for: furthering cyber diplomacy STAKEHOLDER COOPERATION for: coordinate/cooperate in combatting cybercrime STAKEHOLDER COOPERATION for: coordinate/cooperate in preserving multistakeholder internet governance
18:3	2019 - U.S./EU Cyber Dialogue : Joint Elements Statement on the Sixth Summit	2019	The United States and the European Union reaffirmed the importance of the Budapest Convention as a basis for national legislation and international cooperation in fighting cybercrime.	CONFIDENCE BUILDING CBM: adopt legislative basis for combatting cybercrime (i.e., the Budapest Convention)

ID	Document	Document Groups	Quotation Content	Codes
18:4	2019 - U.S./EU Cyber Dialogue : Joint Elements Statement on the Sixth Summit	2019	The United States and European Union are looking forward to the new UN Group of Governmental Experts (GGE) pursuant to the U.S.-drafted resolution on Advancing Responsible State Behaviour in the Context of International Security and the upcoming UN Open Ended Working Group on cyber-related issues and believe that both processes should build upon the landmark 2013 and 2015 consensus reports, including addressing how existing international law applies to State behavior in cyberspace. The U.S. and EU delegations pledged to engage constructively in increasing the international community's awareness, adherence to and implementation of the recommendations contained in the existing consensus GGE reports regarding the applicability of international law to cyberspace, and non-binding norms of responsible behavior by States in cyberspace during peacetime, to which all UN Member States have previously and repeatedly committed.	UNITED NATIONS CBM: the United Nations (UN) may serve as an international body for decision-making, framework creation/implementation, and when developing and adopting universally agreed upon ICT norms/rules/principles (in order to ensure peace and responsible behavior/ICT use) UNITED NATIONS for: following the United Nation's (UN) [2015 and or 2013] GGE report's call for all States to be guided in their use of ICTs in relation to the report
18:5	2019 - U.S./EU Cyber Dialogue : Joint Elements Statement on the Sixth Summit	2019	welcomed important progress on the development and implementation of cyber confidence building measures (CBMs) to reduce misperceptions and the risk of escalation stemming from the use of information and communications technologies. The U.S. and EU delegations noted the importance of the ongoing implementation of the CBMs 10/1/2020 Joint Elements Statement on the Sixth U.S.-EU Cyber Dialogue - United States Department of State https://www.state.gov/joint-elements-statement-on-the-sixth-u-s-eu-cyber-dialogue/ 3/5 committed to in the Organization for Security Cooperation in Europe and welcomed the adoption of cyber CBMs by the Organization for American States and the ASEAN Regional Forum.	CONFIDENCE BUILDING CBM: CBM are important for increasing transparency, predictability, and stability CONFIDENCE BUILDING for: promote cooperation in regional confidence-building measures (CBMs) STAKEHOLDER COOPERATION CBM: cooperation between states/entities (domestic and/or international) is important for furthering economic relationships/development STAKEHOLDER COOPERATION CBM: enhance law enforcement cooperation to reduce incidents that may be misinterpreted as hostile State actions STAKEHOLDER COOPERATION CBM: it is important for other stakeholders such as regional and sub-regional bodies/entities be used to create, promote, and implement CBMs
18:6	2019 - U.S./EU Cyber Dialogue : Joint Elements Statement on the Sixth Summit	2019	In order to keep cyberspace stable and secure, the United States and the European Union are committed to working together and with others to hold States accountable for actions that are contrary to the international consensus on responsible State behavior in cyberspace.	STATE RESPONSIBILITY AND SOVEREIGNTY CBM: hold other nation states / entities accountable for actions that may be contrary to the international consensus on responsible State behavior in cyberspace
19:1	2019 - NATO's London Declaration Official Text	2019	We will continue to increase the resilience of our societies, as well as of our critical infrastructure and our energy security. NATO and Allies, within their respective authority, are committed to ensuring the security of our communications, including 5G, recognising the need to rely on secure and resilient systems.	CRITICAL INFRASTRUCTURE for: promoting resilience (as related to ICTs,cybersecurity, and related critical infrastructure
19:2	2019 - NATO's London Declaration Official Text	2019	We are increasing our tools to respond to cyber attacks, and strengthening our ability to prepare for, deter, and defend against hybrid tactics that seek to undermine our security and societies	CYBER ATTACKS for: strengthen tools and resources needed to prepare, deter, defend, and respond to unlawful use of ICTs, cyber attacks / acts of cyber crime and/or terrorism CYBER STABILITY for: deterring cyber incidents / attacks
20:2	2019 - UN Sec Gen Digital Cooperation Report (final)	2019	Given that human rights apply fully in the digital world, we urge the UN Secretary-General to institute an agencies-wide review of how existing international human rights accords and standards apply to new and emerging digital technologies. Civil society, governments, the private sector and the public should be invited to submit their views on how to apply existing human rights instruments in the digital age in a proactive and transparent process.	HUMAN RIGHTS CBM: domestic and international cooperation amongst nation states, private sector, civil society, and other non-government entities is important in order to strengthen human rights in cyber space / ICT use, etc. HUMAN RIGHTS for: respecting human rights and fundamental freedoms; applying them to cyber space / ICT use, etc.
20:4	2019 - UN Sec Gen Digital Cooperation Report (final)	2019	We believe that autonomous intelligent systems should be designed in ways that enable their decisions to be explained and humans to be accountable for their use. Audits and certification schemes should monitor compliance of artificial intelligence (AI) systems with engineering and ethical standards, which should be developed using multi-stakeholder and multilateral approaches. Life and death decisions should not be delegated to machines. We call for enhanced digital cooperation with multiple stakeholders to think through the design and application of these standards and principles such as transparency and non-bias in autonomous intelligent systems in different social settings.	ARTIFICIAL INTELLIGENCE against: allowing life and death decisions to be delegated to machines ARTIFICIAL INTELLIGENCE CBM: incorporate cooperation through a multistakeholder lense in designing and applying standards and principles (such as transparency and responsibility) towards artificial intelligent systems and related technologies ARTIFICIAL INTELLIGENCE for: holding states/developers/humans responsible for artificial intelligence (AI) systems and their actions

ID	Document	Document Groups	Quotation Content	Codes
20:5	2019 - UN Sec Gen Digital Cooperation Report (final)	2019	Given the wide spectrum of issues, there will of necessity be many forms of digital cooperation; some may be led by the private sector or civil society rather than government or international organisations. Moreover, special efforts are needed to ensure inclusive participation by women and other traditionally marginalised groups in all new or updated methods of global digital cooperation.	INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information STAKEHOLDER COOPERATION CBM: it is important for other stakeholders such as regional and sub-regional bodies/entities be used to create, promote, and implement CBMs
20:6	2019 - UN Sec Gen Digital Cooperation Report (final)	2019	The ultimate purpose of digital technology should always be to improve human welfare. Beyond the socio-economic aspects discussed in the previous chapter, digital technologies have proved that they can connect individuals across cultural and geographic barriers, increasing understanding and potentially helping societies to become more peaceful and cohesive. However, this is only part of the story. There are also many examples of digital technologies being used to violate rights, undermine privacy, polarise societies and incite violence. The questions raised are new, complex and pressing. What are the responsibilities of social media companies, governments and individual users? Who is accountable when data can move across the world in an instant? How can varied stakeholders, in nations with diverse cultural and historical traditions, cooperate to ensure that digital technologies do not weaken human rights but strengthen them?	STATE RESPONSIBILITY AND SOVEREIGNTY CBM: hold other nation states / entities accountable for actions that may be contrary to the international consensus on responsible State behavior in cyberspace
20:7	2019 - UN Sec Gen Digital Cooperation Report (final)	2019	Other existing initiatives on digital security The Paris Call for Trust and Security in Cyberspace is a multi-stakeholder initiative launched in November 2018 and joined by 65 countries, 334 companies – including Microsoft, Facebook, Google and IBM – and 138 universities and non- profit organisations. It calls for measures including coordinated disclosure of technical vulnerabilities. Many leading technology powers, such as the USA, Russia, China, Israel and India, have not signed up.173 The Global Commission on Stability in Cyberspace, an independent multi-stakeholder platform, is developing proposals for norms and policies to enhance international security and stability in cyberspace. The commission has introduced a series of norms, including calls for agreement not to attack critical infrastructure and non-interference in elections, and is currently discussing accountability and the future of cybersecurity. The Global Conference on Cyberspace, also known as the 'London Process', are ad hoc multi-stakeholder conferences held so far in London (2011), Budapest (2012), Seoul (2013), The Hague (2015) and New Delhi (2017). The Global Forum on Cyber Expertise, established after the 2015 Conference, is a platform for identifying best practices and providing support to states, the private sector and organisations in developing cybersecurity frameworks, policies and skills. The Geneva Dialogue on Responsible Behaviour in Cyberspace provides another forum for multi-stakeholder consultation. The Cybersecurity Tech Accord and the Charter of Trust are examples of industry-led voluntary initiatives to identify guiding principles for trust and security, strengthen security of supply chains and improve training of employees in cybersecurity.174	CONFIDENCE BUILDING for: further developement of concepts for international peace and security in the legal use of ICTs (technical and policy level)
20:8	2019 - UN Sec Gen Digital Cooperation Report (final)	2019	The UN's three foundational pillars – peace and security, human rights and development – position it well to help spotlight issues emerging in the digital age and advocate on behalf of humanity's best interests. In our consultations, we heard that despite its well-known weaknesses, the UN retains a unique role and convening power to bring stakeholders together to create the norms and frameworks and assist in developing the capacity we need to ensure a safe and equitable digital future for all people. The UN retains a unique role and convening power to bring stakeholders together to create the norms and frameworks and assist in developing the capacity we need to ensure a safe and equitable digital future for all people.	UNITED NATIONS CBM: the United Nations (UN) may serve as an international body for decision-making, framework creation/implementation, and when developing and adopting universally agreed upon ICT norms/rules/principles (in order to ensure peace and responsible behavior/ICT use)
20:9	2019 - UN Sec Gen Digital Cooperation Report (final)	2019	We recommend that by 2030, every adult should have affordable access to digital networks, as well as digitally-enabled financial and health services, as a means to make a substantial contribution to achieving the SDGs. Provision of these services should guard against abuse by building on emerging principles and best practices, one example of which is providing the ability to opt in and opt out, and by encouraging informed public discourse.	ACCESS for: every adult should have affordable access to digital networks (including digitally-enabled financial and health services)

ID	Document	Document Groups	Quotation Content	Codes
20:10	2019 - UN Sec Gen Digital Cooperation Report (final)	2019	We recommend that a broad, multi-stakeholder alliance, involving the UN, create a platform for sharing digital public goods, engaging talent and pooling data sets, in a manner that respects privacy, in areas related to attaining the SDGs.	STATE RESPONSIBILITY for: dialogue amongst nations by an international body
20:11	2019 - UN Sec Gen Digital Cooperation Report (final)	2019	We call on the private sector, civil society, national governments, multilateral banks and the UN to adopt specific policies to support full digital inclusion and digital equality for women and traditionally marginalised groups. International organisations such as the World Bank and the UN should strengthen research and promote action on barriers women and marginalised groups face to digital inclusion and digital equality	DIGITAL EQUALITY CBM: work towards digital equality and inclusion (i.e., for women and traditionally marginalised groups) - this includes cooperation between the private sector, civil society, and national governments (as well as multilateral banks, and international entities such as the United Nations) STAKEHOLDER COOPERATION for: encourage participation of other stakeholders such as the private sector, academia, and civil society orgs (as appropriate) for CBM and/or norm creation and implementation
20:12	2019 - UN Sec Gen Digital Cooperation Report (final)	2019	We believe that a set of metrics for digital inclusiveness should be urgently agreed, measured worldwide and detailed with sex disaggregated data in the annual reports of institutions such as the UN, the International Monetary Fund, the World Bank, other multilateral development banks and the OECD. From this, strategies and plans of action could be developed.	DIGITAL EQUALITY CBM: create a set of metrics for digital inclusiveness and equality (agreed upon, measured globally, and detailed with specific statistics like gender/sex, nationality, etc). - this would include cooperation amongst an international body (such as the United Nations) as well as the International Monetary Fund (IMF), the World Bank, and other multilateral development banks and [financial] organizations
21:1	2018 - UN Internet Governance Forum (IGF)	2018	Also for the first time in its history, the IGF was convened not as a standalone event but as part of a series of events strategically scheduled by the host country - for Paris Digital Week - that also featured the inaugural events of the Paris Peace Forum and the Govtech Summit. Also unique to IGF 2018, a Head of State, President Macron, launched the “Paris Call for Trust and Security in Cyberspace” -- a framework for regulating the Internet and fighting back against cyber attacks, hate speech and other cyber threats	NORMS CBM: national declarations of adherence to the normative framework of responsible State behavior could build trust and confidence between states
21:2	2018 - UN Internet Governance Forum (IGF)	2018	During the course of the three days, more than 3000 delegates participated in 171 sessions, both onsite and remotely. Paris welcomed participants from 143 different countries. 62% of these were IGF newcomers and 43% were female.	DIGITAL EQUALITY adopted: working towards digital equality and inclusion DIGITAL EQUALITY CBM: work towards digital equality and inclusion (i.e., for women and traditionally marginalised groups) - this includes cooperation between the private sector, civil society, and national governments (as well as multilateral banks, and international entities such as the United Nations)
21:3	2018 - UN Internet Governance Forum (IGF)	2018	Civil Society 45% African Group 25% Government 16% Asia-Pacific Group 16% Intergovernmental Organization 7% Eastern European Group 6% Private Sector 20% Latin American and Caribbean Group (GRULAC) 9% Technical Community 11% Western European and Others Group (WEOG) 38% Press/Media 1% Intergovernmental Organization 6%	STAKEHOLDER COOPERATION for: encourage participation of other stakeholders such as the private sector, academia, and civil society orgs (as appropriate) for CBM and/or norm creation and implementation
21:4	2018 - UN Internet Governance Forum (IGF)	2018	Among the 3000 plus participants, approximately 1000 people participated online. 101 different countries were represented online, with the majority of the participation coming from France, United States, Brazil, Nigeria, United Kingdom, India, Iran, Bangladesh, and Germany.	INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information
21:5	2018 - UN Internet Governance Forum (IGF)	2018	As with many other technologies, these also rely heavily on connectivity -- and the cost and quality of connectivity matter. Having parts of the world that lack basic or broadband connectivity will hinder the ability of these technologies to grow and expand. For these technologies to be at the service of humankind and foster human-centred forms of digitalization, and to avoid undesirable consequences, they must be guided by well-informed, sound and sustainable policies.	ACCESS for: every adult should have affordable access to digital networks (including digitally-enabled financial and health services)
21:6	2018 - UN Internet Governance Forum (IGF)	2018	These include, for example, creating artificial intelligence systems that benefit all people without discrimination, not infringing upon basic human rights, and bringing more transparency in the development of algorithms	CONFIDENCE BUILDING CBM: voluntary transparency PRODUCT for: developers and producers of products and services should take measures to timely mitigate vulnerabilities that are later discovered and be transparent about their process

ID	Document	Document Groups	Quotation Content	Codes
21:7	2018 - UN Internet Governance Forum (IGF)	2018	Not using the term 'fake news', because (i) it is a highly politicized term, often used to express disagreement with accurate information; (ii) it does not fully capture the 'information disorders' that exist, which include false information produced with malicious intent, inaccurate information produced in error, and accurate but misrepresented information. ● Standard-setting for online media sectors - but only with respect to processes (which concern the quality of the product) rather than content (which is a subjective matter). ● Applying ethics and codes of conduct to processes related to new forms of media - just as they are for traditional media outlets - including the algorithms that aggregate online content. ● Establishing networks of reporters and outlets to work together to vet unsourced online stories quickly, to ensure their validity, before reproducing in other networks. ● Valuing journalism and ensuring the safety of journalists. ● Engaging in digital literacy advancement programmes to help audiences discern between good quality and misleading information. ● Promoting better quality online access for people in vulnerable or underserved communities, enabling them to look into information in a more in-depth manner than mobile-only access allows.	STATE RESPONSIBILITY for: establishing a framework / procedures to combat the 'fake news' (maliciously produced false information) phenomenon
21:8	2018 - UN Internet Governance Forum (IGF)	2018	Cyberspace is different, but not separate from, the real world. On the one hand, it is widely accepted that the existing principles that form a sound basis of our world and societies should also be respected as basic principles in Internet governance. On the other hand, specific answers and implementation approaches are needed for new developments and challenges inherent to cyberspace - that by design, is different from the physical space. Digital threats affect the entire Internet ecosystem, and cybersecurity and privacy solutions may have cross-border, cross-disciplinary and cross-sectoral implications. This creates opportunities for legal interoperability and close cooperation between countries,between the developed and developing world and among different stakeholder groups. Cybersecurity measures should protect people. Informed users, aware of the risks and conscious of their behaviour, will take better decisions when participating in online activities. Cybersecurity norms can serve as a mechanism for state and non-state actors to agree on responsible behaviour given that the speed of legislation often struggles to keep up with the pace of changes in the sphere of cybersecurity.	DOMESTIC LAW for: applicability of domestic law to cyber space / ICT usage INTERNATIONAL LAW for: applicability of international law to cyberspace STATE RESPONSIBILITY for: enacting cybersecurity measures that will protect people (privacy, and physical safety, etc) and inform users (transparency)
21:9	2018 - UN Internet Governance Forum (IGF)	2018	There is a need for the global community, including the IGF, to come up with a set of universal values and standards and with that a globally recognized framework that will support the harmonization of these individualistic national approaches.	NORMS CBM: universally agreed upon [voluntary] norms/rules/principles are important for the responsible behavior of States' use of ICTs
21:10	2018 - UN Internet Governance Forum (IGF)	2018	Furthermore, the intersection of the Internet and human rights has evolved to the extent that at the present moment, the public discourse is predominated with the intentional dissemination of inaccurate content in online media, that puts in danger the right to be informed and freedom of expression. Looking at the unregulated online domain, Internet governance has reached the stage where we face an increased proliferation of national laws or regional legal instruments applicable to the Internet public policy	HUMAN RIGHTS for: respecting human rights and fundamental freedoms; applying them to cyber space / ICT use, etc.
22:1	2019 - Russia/India/China 16th Meeting	2019	The Ministers reiterated the importance they attached to the Russia-India-China trilateral format as a platform to foster closer dialogue and practical cooperation in identified areas. As countries with significant international and regional influence, the three countries stand ready to expand mutual consultations and cooperation on international and regional issues of mutual interest in the spirit of mutual respect, respect for sovereignty, non-interference in internal affairs, unity, mutual understanding and trust. The common development and close cooperation of the three countries is conducive for world peace and stability and promoting global growth.	INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information
22:7	2019 - Russia/India/China 16th Meeting	2019	The Ministers reaffirmed their commitment to equal, indivisible common, comprehensive, cooperative and sustainable security. The Ministers reiterated the importance of the role and the need for closer cooperation and consultations in various regional fora and organizations such as the East Asia Summit (EAS), ASEAN Regional Forum (ARF), ASEAN Defence Ministers Meeting Plus (ADMM-Plus), Asia-Europe Meeting (ASEM), the Conference on Interaction and Confidence Building Measures in Asia (CICA) and the Asia Cooperation Dialogue (ACD), to jointly contribute to regional peace, stability, sustainable development and prosperity.	STAKEHOLDER COOPERATION for: support other international and/or regional cooperative partnerships

ID	Document	Document Groups	Quotation Content	Codes
22:11	2019 - Russia/India/China 16th Meeting	2019	The Ministers believed that the United Nations should play a key role on security-related issues in the use of information and communication technologies (ICTs) and welcomed adoption by the UN GA 73-d session of the resolutions “Developments in the Field of Information and Telecommunications in the Context of International Security” and “Countering the use of information and communications technologies for criminal purposes”. They agreed that the UN has a key role in developing universally accepted norms of responsible state behavior in the use of ICTs to ensure a peaceful, secure, open, cooperative, stable, orderly, accessible and equitable ICT environment. They recognized the need for a universal and binding regulatory instrument on combating the criminal use of ICTs in the UN framework and reiterated that all countries should participate in the evolution and functioning of the Internet and its governance on an equal footing. It is important to ensure the inclusiveness and openness of relevant international processes and the fair distribution of basic internet resources, and to build a multilateral, democratic and transparent Internet governance system.They remained committed to working together for the peaceful, secure, open, cooperative and orderly use of ICTs	CONFIDENCE BUILDING CBM: promote the use of ICTs for peaceful purposes NORM for: promote an open, secure, stable, accessible, and peaceful cyber space / ICT environment UNITED NATIONS CBM: the United Nations (UN) may serve as an international body for decision-making, framework creation/implementation, and when developing and adopting universally agreed upon ICT norms/rules/principles (in order to ensure peace and responsible behavior/ICT use)
23:1	2019 - U.S./Japan Seventh Cyber Dialogue	2019	The United States and Japan share a common commitment to ensure an open, interoperable, reliable, and secure cyberspace and to confront emerging cyber challenges	CONFIDENCE BUILDING CBM: promote the use of ICTs for peaceful purposes NORM for: promote an open, secure, stable, accessible, and peaceful cyber space / ICT environment
23:2	2019 - U.S./Japan Seventh Cyber Dialogue	2019	United States and Japan reaffirmed the strength of our alliance partnership and our shared values, which remain the cornerstone of peace, prosperity, and freedom in the Indo- Pacific region	INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information
24:1	2018 - UN Sec Gen disarmament agenda	2018	the United Nations can play a central role in promoting greater understanding of implications posed by developments in science and technology, encouraging responsible innovation and offering mediation in response to incidents of transnational cyberattacks	STATE RESPONSIBILITY for: dialogue amongst nations by an international body
24:2	2018 - UN Sec Gen disarmament agenda	2018	From a legal perspective, there are concerns that some new weapons could challenge existing norms, including international humanitarian law.	HUMAN RIGHTS for: respecting human rights and fundamental freedoms; applying them to cyber space / ICT use, etc.
24:3	2018 - UN Sec Gen disarmament agenda	2018	to ensure its application for peaceful purposes, as well as the responsible dissemination of knowledge, in conformity with the principles and objectives of the United Nations.	CONFIDENCE BUILDING CBM: promote the use of ICTs for peaceful purposes UNITED NATIONS CBM: the United Nations (UN) may serve as an international body for decision-making, framework creation/implementation, and when developing and adopting universally agreed upon ICT norms/rules/principles (in order to ensure peace and responsible behavior/ICT use)
24:4	2018 - UN Sec Gen disarmament agenda	2018	All sides appear to be in agreement that, at a minimum, human oversight over the use of force is necessary	ARTIFICIAL INTELLIGENCE for: holding states/developers/humans responsible for artificial intelligence (AI) systems and their actions
24:5	2018 - UN Sec Gen disarmament agenda	2018	These efforts have made overall progress by elaborating on how international law applies to the use of information and communications technologies by States, as well as on norms, rules and principles of responsible behaviour of States, confdence-building measures and capacity-building.	INTERNATIONAL LAW for: applicability of international law to cyberspace NORMS CBM: universally agreed upon [voluntary] norms/rules/principles are important for the responsible behavior of States' use of ICTs
24:6	2018 - UN Sec Gen disarmament agenda	2018	including that States should not conduct or knowingly support cyberactivity that intentionally damages or otherwise impairs the use and operation of critical infrastructure,	CRITICAL INFRASTRUCTURE against: knowingly damaging critical infrastructure CRITICAL INFRASTRUCTURE against: knowingly support cyberactivity that intentionally damages or impairs the use and operation of critical infrastructure CRITICAL INFRASTRUCTURE for: protecting critical infrastructures
24:7	2018 - UN Sec Gen disarmament agenda	2018	that they should not knowingly allow their territory to be used for internationally wrongful acts using such technology.	STATE RESPONSIBILITY & SOVEREIGNTY against: allowing non-State actors in their territories to unlawfully use ICT
24:8	2018 - UN Sec Gen disarmament agenda	2018	They should also seek ways to support States with limited resources and capacity.	ASSISTANCE CBM: provide assistance and training to developing countries to improve cybsecurity and ICT use CYBER ATTACKS for: strengthen tools and resources needed to prepare, deter, defend, and respond to unlawful use of ICTs, cyber attacks / acts of cyber crime and/or terrorism

ID	Document	Document Groups	Quotation Content	Codes
25:5	2018 - GCSC singapore norms package	2018	commitment by all UN Member States on the duty to prevent and protect against war crimes, genocide, ethnic cleansing and other crimes against humanity. The Ilves Commission helped set the framework for the NETmundial Initiative. The Brandt and Palme Commissions represented important steps both in development and disarmament, respectively. These nongovernmental groups reshaped global discussion of responsible behavior and created new norms for unprecedented international problems.	STAKEHOLDER COOPERATION for: support other international and/or regional cooperative partnerships
25:6	2018 - GCSC singapore norms package	2018	Our proposed norms are therefore intended to accompany and reinforce the eleven norms identifed in the 2013-2015 UN GGE reports.	UNITED NATIONS for: following the United Nation's (UN) [2015 and or 2013] GGE report's call for all States to be guided in their use of ICTs in relation to the report
25:7	2018 - GCSC singapore norms package	2018	“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.”	PRODUCT TAMPERING against: states and non-state actors tampering with products/services (knowingly inserting harmful material into their products) NOR allowing their products to be tampered with
25:9	2018 - GCSC singapore norms package	2018	Those concerned must also reject any apparent state or non- state eforts to compromise products and services, as well as adopt practices that reduce the risk of tampering and permit them to respond if tampering is discovered.	PRODUCT TAMPERING for: rejecting any apparent state or non-state efforts to compromise products/services TAMPERING for: adopt practices that reduce the risk of tampering as well as permit response if tampering is discovered
25:10	2018 - GCSC singapore norms package	2018	“State and non-state actors should not commandeer others’ ICT resources for use as botnets or for similar purposes.”	CYBER ATTACKS against: comandeering the general public's ICT resources for use as botnets or for similar purposes
25:11	2018 - GCSC singapore norms package	2018	“States should create procedurally transparent frameworks to assess whether and when to disclose not publicly known vulnerabilities or faws they are aware of in information systems and technologies. The default presumption should be in favor of disclosure.”	PRODUCT for: creating transparent procedures and frameworks to asses whether and when to disclose not publicly known vulnerabilities or flaws in their information systems and/or technologies
25:12	2018 - GCSC singapore norms package	2018	“Developers and producers of products and services on which the stability of cyberspace depends should prioritize security and stability, take reasonable steps to ensure that their products or services are free from signifcant vulnerabilities, take measures to timely mitigate vulnerabilities that are later discovered and to be transparent about their process. All actors have a duty to share information on vulnerabilities in order to help prevent or mitigate malicious cyber activity.”	PRODUCT for: developers and producers of products and services should prioritize security and stability PRODUCT for: developers and producers of products and services should take measures to timely mitigate vulnerabilities that are later discovered and be transparent about their process
25:13	2018 - GCSC singapore norms package	2018	“States should enact appropriate measures, including laws and regulations, to ensure basic cyber hygiene.	STATE RESPONSIBILITY for: nation-state enacted laws and/or regulations to ensure basic cyber protocols/cleanliness/hygiene
25:14	2018 - GCSC singapore norms package	2018	“Non-state actors should not engage in ofensive cyber operations and state actors should prevent and respond to such activities if they occur.”	STATE RESPONSIBILITY & SOVEREIGNTY against: allowing non-State actors in their territories to unlawfully use ICT STATE RESPONSIBILITY for: responding to offensive/illegal/unlawful cyber activities by non state actors if/when discovered
25:15	2018 - GCSC singapore norms package	2018	Without prejudice to their rights and obligations, state and non-state actors should not conduct or 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.16	CYBER STABILITY for: protecting the public core of the internet NORM against: states and non-state actors conducting activity that intentionally and substantially damages the general availability or integrity of the public core of the internet
25:16	2018 - GCSC singapore norms package	2018	State and non-state actors should not pursue, support or allow cyber operations intended to disrupt the technical infrastructure essential to elections, referenda or plebiscites.	CYBER ATTACKS against: conducting ICT operations intended to disrupt essential infrastructure of political processes (i.e., election processes) CYBER STABILITY for: protecting political systems
26:1	2018 - Charter of Trust	2018	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”.	STATE RESPONSIBILITY AND SOVEREIGNTY CBM: hold other nation states / entities accountable for actions that may be contrary to the international consensus on responsible State behavior in cyberspace
26:2	2018 - Charter of Trust	2018	Companies – and if necessary – governments must establish risk-based rules that ensure adequate protections across all IoT layers with clearly defined and mandatory requirements. Ensure confidentiality, authenticity, integrity and availability by setting baseline standards such as	CONFIDENCE BUILDING for: ensure confidentiality, authenticity, integrity, and availability of a secure digital world CONFIDENCE BUILDING for: establish risk-based rules that ensure adequate protections with clearly defined and mandatory requirements.
26:3	2018 - Charter of Trust	2018	Identity and access management: Connected devices must have secure identities and safe-guarding measures that only grant access to authorized users and devices – 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	PRODUCT for: developers must strive to create secure products for society; such products will require consistent updates and improvements upon security; products must work as developers claim they will (i.e., confidentiality based encryption/data-storage/transmission)

ID	Document	Document Groups	Quotation Content	Codes
26:4	2018 - Charter of Trust	2018	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	EDUCATION for: include cybersecurity courses in school curricula (i.e., primary school, degree courses in undergrad, professional education, and trainings
26:5	2018 - Charter of Trust	2018	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	EDUCATION (CERTIFICATION) for: companies and governments (if necessary) should establish h mandatory, independent, third-party certifications
26:6	2018 - Charter of Trust	2018	Participate in an industrial cybersecurity network in order to share new insights, information on incidents et al.; report incidents beyond today's practice, which focuses on critical infrastructure	CRITICAL INFRASTRUCTURE for: promoting resilience (as related to ICTs,cybersecurity, and related critical infrastructure CRITICAL INFRASTRUCTURE for: protecting critical infrastructures INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information PRODUCT for: developers and producers of products and services should take measures to timely mitigate vulnerabilities that are later discovered and be transparent about their process
26:7	2018 - Charter of Trust	2018	Promote multilateral collaborations in regulation and standardization to set a level playing field matching the global reach of WTO; inclusion of rules for cybersecurity into Free Trade Agreements (FTAs)	STAKEHOLDER COOPERATION CBM: form bilateral and multilateral cooperation initiatives to build on established partnerships/relationships STAKEHOLDER COOPERATION CBM: states should participate and cooperate in multilateral forums
27:1	2018 - Cybersecurity Tech Accord _ Cybersecurity Tech Accord	2018	We will strive to protect all our users and customers from cyberattacks – whether an individual, organization or government – irrespective of their technical acumen, culture or location, or the motives of the attacker, whether criminal or geopolitical.	STATE RESPONSIBILITY for: protecting users/customers from cyberattacks, regardless who the victim is
27:2	2018 - Cybersecurity Tech Accord _ Cybersecurity Tech Accord	2018	We will design, develop, and deliver products and services that prioritize security, privacy, integrity and reliability, and in turn reduce the likelihood, frequency, exploitability, and severity of vulnerabilities.	PRODUCT for: developers and producers of products and services should prioritize security and stability
27:3	2018 - Cybersecurity Tech Accord _ Cybersecurity Tech Accord	2018	We will protect against tampering with and exploitation of technology products and services during their development, design, distribution and use.	PRODUCT TAMPERING against: states and non-state actors tampering with products/services (knowingly inserting harmful material into their products) NOR allowing their products to be tampered with TAMPERING for: adopt practices that reduce the risk of tampering as well as permit response if tampering is discovered
27:4	2018 - Cybersecurity Tech Accord _ Cybersecurity Tech Accord	2018	We will not help governments launch cyberattacks against innocent citizens and enterprises from anywhere.	CYBER ATTACKS against: states helping governments launch cyberattacks against innocent civilians/other innocents NON-STATE RESPONSIBILITY for: responsibilities should be imposed on non-state actos as well (regarding lawful use of ICTs, cybersecurity, maintaining stability and international security/peace, etc.)
27:5	2018 - Cybersecurity Tech Accord _ Cybersecurity Tech Accord	2018	We will provide our users, customers and the wider developer ecosystem with information and tools that enable them to understand current and future threats and protect themselves against them.	EDUCATE AND STRENGTHEN THE GENERAL PUBLIC for: providing users/customers/the general public with information and tools that will enable them to understand current and future threats, as well as protect against them
27:6	2018 - Cybersecurity Tech Accord _ Cybersecurity Tech Accord	2018	We will support civil society, governments and international organizations in their efforts to advance security in cyberspace and to build cybersecurity capacity in developed and emerging economies alike.	ASSISTANCE CBM: provide assistance and training to developing countries to improve cybsecurity and ICT use
27:7	2018 - Cybersecurity Tech Accord _ Cybersecurity Tech Accord	2018	We will work with each other and will establish formal and informal partnerships with industry, civil society, and security researchers, across proprietary and open source technologies to improve technical collaboration, coordinated vulnerability disclosure, and threat sharing, as well as to minimize the levels of malicious code being introduced into cyberspace.	INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information STAKEHOLDER COOPERATION for: encourage participation of other stakeholders such as the private sector, academia, and civil society orgs (as appropriate) for CBM and/or norm creation and implementation
27:8	2018 - Cybersecurity Tech Accord _ Cybersecurity Tech Accord	2018	We will encourage global information sharing and civilian efforts to identify, prevent, detect, respond to, and recover from cyberattacks and ensure flexible responses to security of the wider global technology ecosystem.	INFORMATION EXCHANGE for: encourage global information sharing and civilian efforts to identify, prevent, detect, respond to, and/or recover from cyberattacks
28:1	2018 - paris call	2018	We reaffirm our support to an open, secure, stable, accessible and peaceful cyberspace, which has become an integral component of life in all its social, economic, cultural and political aspects.	NORM for: promote an open, secure, stable, accessible, and peaceful cyber space / ICT environment

ID	Document	Document Groups	Quotation Content	Codes
28:2	2018 - paris call	2018	We also reaffirm that international law, including the United Nations Charter in its entirety, international humanitarian law and customary international law is applicable to the use of information and communication technologies (ICT) by States	HUMAN RIGHTS for: respecting human rights and fundamental freedoms; applying them to cyber space / ICT use, etc. INTERNATIONAL LAW for: applicability of international law to cyberspace STATE RESPONSIBILITY for: adhering to rules and regulations agreed upon by previously enacted international law/mandates/treaties
28:3	2018 - paris call	2018	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.	HUMAN RIGHTS for: applicability of international human rights law(s) to cyberspace
28:4	2018 - paris call	2018	together with the voluntary norms of responsible State behavior during peacetime and associated confidence and capacity-building measures developed within the United Nations, is the foundation for international peace and security in cyberspace.	STATE RESPONSIBILITY for: states should behave responsibly in cyberspace (and use ICTs responsibly) during peacetime UNITED NATIONS CBM: the United Nations (UN) may serve as an international body for decision-making, framework creation/implementation, and when developing and adopting universally agreed upon ICT norms/rules/principles (in order to ensure peace and responsible behavior/ICT use)
28:5	2018 - paris call	2018	We condemn malicious cyber activities in peacetime, notably the ones threatening or resulting in significant, indiscriminate or systemic harm to individuals and critical infrastructure and welcome calls for their improved protection.	CRITICAL INFRASTRUCTURE against: knowingly damaging critical infrastructure CRITICAL INFRASTRUCTURE for: protecting critical infrastructures
28:6	2018 - paris call	2018	We also welcome efforts by States and non-state actors to provide support to victims of malicious use of ICTs on an impartial and independent basis, whenever it occurs, whether during or outside of armed conflict.	STATE RESPONSIBILITY & SOVEREIGNTY for: encourage states and non-state actors to provide support to victims of malicious use of ICTs (impartial and independent basis)
28:7	2018 - paris call	2018	We recognize the responsibilities of key private sector actors in improving trust, security and stability in cyberspace and encourage initiatives aimed at strengthening the security of digital processes, products and services.	STAKEHOLDER COOPERATION for: recognizing the private sector's responsibilities in working towards improving trust, security, and stability in cyberspace
28:8	2018 - paris call	2018	We welcome collaboration among governments, the private sector and civil society to create new cybersecurity standards that enable infrastructures and organizations to improve cyber protections.	INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information STAKEHOLDER COOPERATION for: encourage participation of other stakeholders such as the private sector, academia, and civil society orgs (as appropriate) for CBM and/or norm creation and implementation
28:9	2018 - paris call	2018	We underline the need to enhance broad digital cooperation and increase capacity-building efforts by all actors and encourage initiatives that build user resilience and capabilities.	CAPACITY BUILDING CBM: encourage further work in capacity-building CYBERSPACE STABILITY for: state and non-state actors (including international entities) should increase efforts to build capacity and capabilities (i.e., train staff) and promote a shared understanding of the importance of the stability of cyberspace
28:10	2018 - paris call	2018	strengthened multistakeholder approach and of additional efforts to reduce risks to the stability of cyberspace and to build-up confidence, capacity and trust.	STAKEHOLDER COOPERATION for: establishing a standing multistakeholder engagement mechanism in order to address stability issues (this includes adequate involvement and consultation of states, non-state actors such as private sector entities, and civil society)
28:11	2018 - paris call	2018	Strengthen our capacity to prevent malign interference by foreign actors aimed at undermining electoral processes through malicious cyber activities;	CRITICAL INFRASTRUCTURE for: protecting critical infrastructures CYBER ATTACKS against: conducting ICT operations intended to disrupt essential infrastructure of political processes (i.e., election processes) CYBER STABILITY for: protecting political systems
28:12	2018 - paris call	2018	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;	CYBER ATTACK for: preventing ICT-enabled theft of intellectual property (this includes trade secrets and other confidential business information)
28:13	2018 - paris call	2018	Develop ways to prevent the proliferation of malicious ICT tools and practices intended to cause harm;	CYBER STABILITY for: develop a framework/rules/protocols intended to help prevent the use of ICT tools/practices that are intended to cause harm in order to keep cyberspace secure
28:14	2018 - paris call	2018	Support efforts to strengthen an advanced cyber hygiene for all actors;	STATE RESPONSIBILITY for: nation-state enacted laws and/or regulations to ensure basic cyber protocols/cleanliness/hygiene

ID	Document	Document Groups	Quotation Content	Codes
28:15	2018 - paris call	2018	Promote the widespread acceptance and implementation of international norms of responsible behavior as well as confidence-building measures in cyberspace.	CYBERSPACE STABILITY for: both nation states and non-state actors must adopt and implement norms that increase the stabilitiy of cyberspace (promoting restraint and encouraging action) NORMS CBM: national declarations of adherence to the normative framework of responsible State behavior could build trust and confidence between states NORMS CBM: universally agreed upon [voluntary] norms/rules/principles are important for the responsible behavior of States' use of ICTs
30:1	2018 - ASEAN AMCC-Chairmans-Statement-Finalised	2018	AMCC participants welcomed the adoption of the ASEAN Leaders' Statement on Cybersecurity Cooperation by ASEAN Leaders at the 32nd ASEAN Summit in April 2018, in recognition of the growing urgency and sophistication of transboundary cyber threats.	STATE RESPONSIBILITY for: adhering to rules and regulations agreed upon by previously enacted international law/mandates/treaties
30:2	2018 - ASEAN AMCC-Chairmans-Statement-Finalised	2018	In response to ASEAN Leaders' direction to closely consider and submit recommendations on feasible options of coordinating ASEAN cybersecurity efforts among various platforms of the three pillars of ASEAN, AMCC participants agreed that there is a need for a formal ASEAN cybersecurity mechanism to consider and to decide on inter-related cyber diplomacy, policy and operational issues.	CAPACITY BUILDING CBM: develop regional approaches to capacity-building CONFIDENCE BUILDING for: promote cooperation in regional confidence-building measures (CBMs) STAKEHOLDER COOPERATION CBM: it is important for other stakeholders such as regional and sub-regional bodies/entities be used to create, promote, and implement CBMs STAKEHOLDER COOPERATION for: establishing a standing multistakeholder engagement mechanism in order to address stability issues (this includes adequate involvement and consultation of states, non-state actors such as private sector entities, and civil society)
30:3	2018 - ASEAN AMCC-Chairmans-Statement-Finalised	2018	11 voluntary, non-binding norms recommended in the 2015 Report of the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UNGGE), as well as to focus on regional capacity-building in implementing these norm	UNITED NATIONS for: following the United Nation's (UN) [2015 and or 2013] GGE report's call for all States to be guided in their use of ICTs in relation to the report
30:4	2018 - ASEAN AMCC-Chairmans-Statement-Finalised	2018	Participants expressed in-principle support on the need to establish the ASEAN Directory of Cyber Points-of-Contact.	CONFIDENCE BUILDING CBM: establishing national/international/regional/sub-regional Points of Contact (POCs) is a CBM as well as a prerequisite for the implementation of many other CBMs (i.e., useful for diplomatic, policy, legal and technical exchanges, as well as incident reporting and responses)
32:1	2018 - Australian Prime Minister Malcolm Turnbull meets with Australia-US Cyber Security experts in Washington _ Australian Strategic Policy Institute _ ASPI	2018	Cooperation with likeminded countries is the best way to improve cybersecurity, and cooperation between the U.S. and Australia is crucial for security in the Asia Pacific region	INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information
32:2	2018 - Australian Prime Minister Malcolm Turnbull meets with Australia-US Cyber Security experts in Washington _ Australian Strategic Policy Institute _ ASPI	2018	deter and respond to unacceptable behavior in cyberspace – particularly by states and their proxies	CYBERSPACE STABILITY for: both nation states and non-state actors must adopt and implement norms that increase the stabilitiy of cyberspace (promoting restraint and encouraging action) INFORMATION EXCHANGE AND TRANSPARENCY for: cooperate/exchange guidelines and/or best practices against disruptions by non-State actors
32:3	2018 - Australian Prime Minister Malcolm Turnbull meets with Australia-US Cyber Security experts in Washington _ Australian Strategic Policy Institute _ ASPI	2018	and how to strengthen coordination between government and the private sector	STAKEHOLDER COOPERATION for: encourage participation of other stakeholders such as the private sector, academia, and civil society orgs (as appropriate) for CBM and/or norm creation and implementation STAKEHOLDER COOPERATION for: establishing a standing multistakeholder engagement mechanism in order to address stability issues (this includes adequate involvement and consultation of states, non-state actors such as private sector entities, and civil society) STAKEHOLDER COOPERATION for: recognizing the private sector's responsibilities in working towards improving trust, security, and stability in cyberspace

ID	Document	Document Groups	Quotation Content	Codes
33:1	2019 Third Australia-India Cyber Policy Dialogue _ DFAT	2019	India and Australia affirmed commitment to ensure security and stability in cyberspace underpinned by their shared commitment to the implementation of the UNGGE reports of the 2013 and 2015	UNITED NATIONS for: following the United Nation's (UN) [2015 and or 2013] GGE report's call for all States to be guided in their use of ICTs in relation to the report
33:2	2019 Third Australia-India Cyber Policy Dialogue _ DFAT	2019	application of international law	INTERNATIONAL LAW for: applicability of international law to cyberspace
33:3	2019 Third Australia-India Cyber Policy Dialogue _ DFAT	2019	in particular the UN Charter,	STATE RESPONSIBILITY for: adhering to rules and regulations agreed upon by previously enacted international law/mandates/treaties
33:4	2019 Third Australia-India Cyber Policy Dialogue _ DFAT	2019	agreed norms of responsible state behavior	NORMS CBM: universally agreed upon [voluntary] norms/rules/principles are important for the responsible behavior of States' use of ICTs
33:5	2019 Third Australia-India Cyber Policy Dialogue _ DFAT	2019	Both countries are committed to constructive dialogue on these issues in multilateral forums including the UN Group of Governmental Experts and Open Ended Working Group.	INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information STAKEHOLDER COOPERATION CBM: states should participate and cooperate in multilateral forums UNITED NATIONS CBM: the United Nations (UN) may serve as an international body for decision-making, framework creation/implementation, and when developing and adopting universally agreed upon ICT norms/rules/principles (in order to ensure peace and responsible behavior/ICT use)
33:6	2019 Third Australia-India Cyber Policy Dialogue _ DFAT	2019	Noting the need to strengthen bilateral engagement on cyber security and technology policy issues, India and Australia agreed to further enhance practical cyber security policy cooperation through reciprocal expert exchanges to share information on cyber security policy development, telecommunications, legislative developments, and engagement with the private sector.	INFORMATION EXCHANGE CBM: encouraging exchanges between research and academic institutions INFORMATION EXCHANGE CBM: exchange national views on the use of ICTS in conflicts STAKEHOLDER COOPERATION CBM: exchange of personnel STAKEHOLDER COOPERATION for: encourage participation of other stakeholders such as the private sector, academia, and civil society orgs (as appropriate) for CBM and/or norm creation and implementation STAKEHOLDER COOPERATION for: recognizing the private sector's responsibilities in working towards improving trust, security, and stability in cyberspace
33:7	2019 Third Australia-India Cyber Policy Dialogue _ DFAT	2019	Both countries acknowledge that greater international cooperation is required to address the cyber security risks currently posed by insecure IoT devices and shape and align security standards for IoT devices globally	INFORMATION EXCHANGE for: increasing international cooperation is required to address cyber security risks
33:8	2019 Third Australia-India Cyber Policy Dialogue _ DFAT	2019	Both countries noted that the increasing ubiquity of the Internet of Things (IoT) provides significant opportunities and benefits for our respective economies, including through the development of Smart Cities. Capitalising on these opportunities relies on security being built in by design.	PRODUCT for: developers and producers of products and services should prioritize security and stability
34:1	2018 - Second Australia-Indonesia Cyber Policy Dialogue _ DFAT	2018	Australia and Indonesia discussed their shared interests in an open, free and secure Internet that supports economic growth and innovation.	NORM for: supporting a free and secure internet / cyber space that supports economic growth and innovation
34:2	2018 - Second Australia-Indonesia Cyber Policy Dialogue _ DFAT	2018	Australia and Indonesia reaffirmed their commitment to promote international stability for cyberspace based on existing international law	INTERNATIONAL LAW for: applicability of international law to cyberspace
34:3	2018 - Second Australia-Indonesia Cyber Policy Dialogue _ DFAT	2018	voluntary and non-binding norms of responsible behaviour,	NORMS CBM: universally agreed upon [voluntary] norms/rules/principles are important for the responsible behavior of States' use of ICTs
34:4	2018 - Second Australia-Indonesia Cyber Policy Dialogue _ DFAT	2018	practical confidence building measures	CONFIDENCE BUILDING for: develop and implement [practical] cyber confidence building measures (CBMs) between nation states
34:5	2018 - Second Australia-Indonesia Cyber Policy Dialogue _ DFAT	2018	cooperative capacity building	CAPACITY BUILDING CBM: encourage further work in capacity-building
34:6	2018 - Second Australia-Indonesia Cyber Policy Dialogue _ DFAT	2018	Australia and Indonesia reaffirmed that existing international law applies to states' activities in cyberspace and that the UN Charter applies to states' activities in cyberspace	STATE RESPONSIBILITY for: adhering to rules and regulations agreed upon by previously enacted international law/mandates/treaties

ID	Document	Document Groups	Quotation Content	Codes
34:7	2018 - Second Australia-Indonesia Cyber Policy Dialogue _ DFAT	2018	They agreed to continue to promote the set of common voluntary and non-binding norms of responsible state behaviour recommended in the 2015 UNGGE report, and committed to act in accordance with these norms.	UNITED NATIONS for: following the United Nation's (UN) [2015 and or 2013] GGE report's call for all States to be guided in their use of ICTs in relation to the report
34:8	2018 - Second Australia-Indonesia Cyber Policy Dialogue _ DFAT	2018	hey noted the urgent need to cooperate together and with other regional partners on measures to reduce risk in cyberspace.	CONFIDENCE BUILDING for: promote cooperation in regional confidence-building measures (CBMs) STAKEHOLDER COOPERATION CBM: form bilateral and multilateral cooperation initiatives to build on established partnerships/relationships STAKEHOLDER COOPERATION CBM: states should participate and cooperate in multilateral forums
35:2	2018 - ASEAN co-chairs-summary-report-of-1st-ism-on-icts-security-final	2018	to provide a forum for dialogue and to assess common and basic regional needs for capacity building on ICTs Security;	CAPACITY BUILDING CBM: develop regional approaches to capacity-building INFORMATION EXCHANGE CBM: exchange national views on the use of ICTS in conflicts INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information
35:3	2018 - ASEAN co-chairs-summary-report-of-1st-ism-on-icts-security-final	2018	CBM #1: Establishment of ARF Points of Contact (POC) Directory on Security of and in the Use of ICTs (Co-Lead Countries: Malaysia and Australia)	CONFIDENCE BUILDING CBM: establishing national/international/regional/sub-regional Points of Contact (POCs) is a CBM as well as a prerequisite for the implementation of many other CBMs (i.e., useful for diplomatic, policy, legal and technical exchanges, as well as incident reporting and responses)
35:4	2018 - ASEAN co-chairs-summary-report-of-1st-ism-on-icts-security-final	2018	CBM #2: Sharing of Information on National Laws, Policies, Best Practices and Strategies as well as Rules and Regulations (Co-Lead Countries: Japan and the Philippines),	INFORMATION EXCHANGE for: sharing information regarding national laws/policies/rules/regulations regarding ICTs/cyber space/cybersecurity INFORMATION EXCHANGE for: sharing of good/best practices in relation to ICTs and cybersecurity
35:5	2018 - ASEAN co-chairs-summary-report-of-1st-ism-on-icts-security-final	2018	which aims to reduce misunderstanding and miscalculation and prevent possible conflicts by increasing transparency through sharing information of each ARF Participating Country's system.	CONFIDENCE BUILDING for: CBMs' value in increasing transparency, predictability, and stability
35:6	2018 - ASEAN co-chairs-summary-report-of-1st-ism-on-icts-security-final	2018	Protection of Critical Infrastructures and Consultations Mechanism (Co-Lead Countries: European Union and Singapore)	CRITICAL INFRASTRUCTURE for: protecting critical infrastructures
35:7	2018 - ASEAN co-chairs-summary-report-of-1st-ism-on-icts-security-final	2018	Awareness-Raising and Information Sharing on Emergency Responses to Security Incidents in the Use of ICTs (Lead Country: China),	STAKEHOLDER COOPERATION CBM: states should support/facilitate cooperation amongst national response teams and other relevant entities
35:8	2018 - ASEAN co-chairs-summary-report-of-1st-ism-on-icts-security-final	2018	As an effort to overcome this challenge, the Meeting noted that there had been a recommendation for the ADMM-Plus members to undertake exercises and workshops focusing on cyber law, as well as to review the possibility of establishing FINAL Co-Chairs' Summary Report of the 1st ARF ISM on ICTs Security Kuala Lumpur, Malaysia, 25-26 April 2018 Page 7 of 8 a CERT or Computer Incidents Response Team (CIRT) under the ADMM-Plus framework.	EMERGENCY RESPONSE CBM: develop guidance on scenario-based exercises at the policy, operational, and technical level between nation states and their Computer Emergency Response Teams (CERTs) and/or Computer Security Incident Response Teams (CSIRTs) EMERGENCY RESPONSE CBM: each state/regional partnership should establish and/or strengthen a national computer emergency response team (CERT) / cybersecurity incident response team
35:10	2018 - ASEAN co-chairs-summary-report-of-1st-ism-on-icts-security-final	2018	to promote cooperation among all stakeholders including governments, organisations, and private entities to better utilise best-practices models in assessing national status and progress in the implementation of cybersecurity policies; and	STAKEHOLDER COOPERATION for: encourage participation of other stakeholders such as the private sector, academia, and civil society orgs (as appropriate) for CBM and/or norm creation and implementation
35:11	2018 - ASEAN co-chairs-summary-report-of-1st-ism-on-icts-security-final	2018	to strengthen capacity building and promote technical cooperation and confidence- building measures under the ambit of the ISM on ICTs Security.	CYBERSPACE STABILITY for: state and non-state actors (including international entities) should increase efforts to build capacity and capabilities (i.e., train staff) and promote a shared understanding of the importance of the stability of cyberspace
36:1	2018 - The Sixth U.S.-Japan Cyber Dialogue - United States Department of State	2018	The United States and Japan share a common commitment to ensure an open, interoperable, reliable, and secure cyberspace and confront emerging cyber challenges	NORM for: promote an open, secure, stable, accessible, and peaceful cyber space / ICT environment
36:2	2018 - The Sixth U.S.-Japan Cyber Dialogue - United States Department of State	2018	including our shared commitment to deter cyber adversaries and malicious cyber activities	CYBER STABILITY for: deterring cyber incidents / attacks

ID	Document	Document Groups	Quotation Content	Codes
36:3	2018 - The Sixth U.S.-Japan Cyber Dialogue - United States Department of State	2018	protect the cybersecurity of critical infrastructure	CRITICAL INFRASTRUCTURE for: protecting critical infrastructures
36:4	2018 - The Sixth U.S.-Japan Cyber Dialogue - United States Department of State	2018	address international security issues in cyberspace	CONFIDENCE BUILDING CBM: address issues [related to cyber space/cybersecurity/ICTs]
36:5	2018 - The Sixth U.S.-Japan Cyber Dialogue - United States Department of State	2018	reaffirmed their shared commitment to cooperate on cyber issues in relevant multilateral venues, including the United Nations and the ASEAN Regional Forum.	INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information STAKEHOLDER COOPERATION CBM: states should participate and cooperate in multilateral forums
37:1	2018 - Singapore Signs Memorandum of Understanding with Canada on Cybersecurity Cooperation	2018	information exchange and sharing on cyber threats and cyber-attacks	INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information
37:2	2018 - Singapore Signs Memorandum of Understanding with Canada on Cybersecurity Cooperation	2018	sharing of best practices on human resource development	CONFIDENCE BUILDING for: promote human resource development (as related to cyber space, ICTs, cybersecurity, etc.)
37:3	2018 - Singapore Signs Memorandum of Understanding with Canada on Cybersecurity Cooperation	2018	provision of technical and certification services and development of cybersecurity standards;	INFORMATION EXCHANGE for: sharing of good/best practices in relation to ICTs and cybersecurity
37:4	2018 - Singapore Signs Memorandum of Understanding with Canada on Cybersecurity Cooperation	2018	collaboration on regional cybersecurity capacity building.	CAPACITY BUILDING CBM: develop regional approaches to capacity-building
37:5	2018 - Singapore Signs Memorandum of Understanding with Canada on Cybersecurity Cooperation	2018	including critical infrastructure protection,	CRITICAL INFRASTRUCTURE for: protecting critical infrastructures
37:6	2018 - Singapore Signs Memorandum of Understanding with Canada on Cybersecurity Cooperation	2018	enhance Singapore's ongoing domestic cybersecurity ecosystem development efforts	CONFIDENCE BUILDING for: promote the cybersecurity ecosystem
37:7	2018 - Singapore Signs Memorandum of Understanding with Canada on Cybersecurity Cooperation	2018	advance the development of a secure and trusted regional cyberspace in ASEAN.	CYBER STABILITY for: maintaining a secure, safe, and trustable ICT environment
38:1	2018 - Singapore Signs MOU Extension with India to Continue Cybersecurity Cooperation	2018	extend cooperation between the Singapore Computer Emergency Response Team (SingCERT) and the Indian Computer Emergency Response Team (CERT-In) for an additional period of five years	EMERGENCY RESPONSE CBM: each state/regional partnership should establish and/or strengthen a national computer emergency response team (CERT) / cybersecurity incident response team STAKEHOLDER COOPERATION CBM: states should support/facilitate cooperation amongst national response teams and other relevant entities
38:2	2018 - Singapore Signs MOU Extension with India to Continue Cybersecurity Cooperation	2018	establishment of a formal framework for professional dialogue	INFORMATION EXCHANGE for: establish a formal framework to facilitate professional dialogue
38:3	2018 - Singapore Signs MOU Extension with India to Continue Cybersecurity Cooperation	2018	collaboration on cyber security technology and research related to smart technologies	INFORMATION EXCHANGE CBM: encouraging exchanges between research and academic institutions
38:4	2018 - Singapore Signs MOU Extension with India to Continue Cybersecurity Cooperation	2018	exchange of best practices;	INFORMATION EXCHANGE for: sharing of good/best practices in relation to ICTs and cybersecurity

ID	Document	Document Groups	Quotation Content	Codes
38:5	2018 - Singapore Signs MOU Extension with India to Continue Cybersecurity Cooperation	2018	professional exchanges of human resource development.	CONFIDENCE BUILDING for: promote human resource development (as related to cyber space, ICTs, cybersecurity, etc.)
39:1	2018 - Singapore Signs Memorandum of Cooperation on Cybersecurity Capacity Building with the United Kingdom	2018	capacity building programmes to Commonwealth Member States for a two- year period beginning September 2018	CAPACITY BUILDING CBM: encourage further work in capacity-building INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information STATE RESPONSIBILITY for: adhering to rules and regulations agreed upon by previously enacted international law/mandates/treaties
39:2	2018 - Singapore Signs Memorandum of Cooperation on Cybersecurity Capacity Building with the United Kingdom	2018	It presents an opportunity for both countries to share expertise and resources	INFORMATION EXCHANGE for: share expertise and resources (regarding ICTs/cyber space/cybersecurity, etc.)
40:1	2018 - 10th BRICS Summit Johannesburg Declaration	2018	We recommit ourselves to a world of peace and stability, and support the central role of the United Nations, the purposes and principles enshrined in the UN Charter and respect for international law, promoting democracy and the rule of law.	STATE RESPONSIBILITY for: adhering to rules and regulations agreed upon by previously enacted international law/mandates/treaties
40:2	2018 - 10th BRICS Summit Johannesburg Declaration	2018	strengthen multilateralism and the rule of law in international relations, and to promote a fair, just, equitable, democratic and representative international order.	STAKEHOLDER COOPERATION CBM: states should participate and cooperate in multilateral forums
40:3	2018 - 10th BRICS Summit Johannesburg Declaration	2018	we stress the importance of international cooperation against terrorist and criminal use of ICTs and therefore reiterate the need to develop a universal regulatory binding instrument on combatting the criminal use of ICTs within the UN	CYBER ATTACKS for: strengthen tools and resources needed to prepare, deter, defend, and respond to unlawful use of ICTs, cyber attacks / acts of cyber crime and/or terrorism INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information STAKEHOLDER COOPERATION for: work / intensify cooperation against criminal/terrorist use of ICTs UNITED NATIONS CBM: the United Nations (UN) may serve as an international body for decision-making, framework creation/implementation, and when developing and adopting universally agreed upon ICT norms/rules/principles (in order to ensure peace and responsible behavior/ICT use)
40:4	2018 - 10th BRICS Summit Johannesburg Declaration	2018	We also acknowledge the importance to establish a framework of cooperation among BRICS member States on ensuring security in the Use of ICTs and, in this regard, BRICS member States will work towards consideration and elaboration of a BRICS intergovernmental agreement on cooperation on this matter.	INFORMATION EXCHANGE for: establish a formal framework to facilitate professional dialogue NORMS CBM: national declarations of adherence to the normative framework of responsible State behavior could build trust and confidence between states
40:5	2018 - 10th BRICS Summit Johannesburg Declaration	2018	n this regard, we commit to continue to work together through the existing mechanisms to contribute to the secure, open, peaceful, cooperative and orderly use of ICTs 10/7/2020 10th BRICS Summit Johannesburg Declaration https://www.mea.gov.in/bilateral-documents.htm?dtl/30190/10th_BRICS_Summit_Johannesburg_Declaration 10/20 on the basis of participation by all states on an equal footing in the evolution and functioning of the internet and its governance, bearing in mind the need to involve the relevant stakeholders in their respective roles and responsibilities.	NORM for: promote an open, secure, stable, accessible, and peaceful cyber space / ICT environment STAKEHOLDER COOPERATION for: coordinate/cooperate in preserving multistakeholder internet governance
40:6	2018 - 10th BRICS Summit Johannesburg Declaration	2018	We recognise the critical and positive role the internet plays globally in promoting economic, social and cultural development	NORM for: supporting a free and secure internet / cyber space that supports economic growth and innovation STAKEHOLDER COOPERATION CBM: cooperation between states/entities (domestic and/or international) is important for furthering economic relationships/development
40:7	2018 - 10th BRICS Summit Johannesburg Declaration	2018	We recognise the importance of the development and transfer of technologies, including to developing countries, contributing to long- term sustainable and balanced global growth, and in this regard stress the importance of strengthening cooperation in intellectual property rights which contributes to innovation and the advent of new technologies to the beneft of society as a whole	ASSISTANCE CBM: provide assistance and training to developing countries to improve cybsecurity and ICT use

ID	Document	Document Groups	Quotation Content	Codes
40:8	2018 - 10th BRICS Summit Johannesburg Declaration	2018	Appropriate policies and measures need to be taken to ensure that the developing countries beneft from the advantages of technological progress and do not sufer from lack of its early adoption.	ASSIST for: adopting appropriate policies and measures so that developing countries benefit from the advantages of technological progress (and do not suffer from lack of early adoption)
40:9	2018 - 10th BRICS Summit Johannesburg Declaration	2018	It is essential to develop efective policies to bridge the digital divides, including through supporting people to learn and by adopting new technologies and ensure efective mechanisms for transfer of relevant technologies.	ASSISTANCE CBM: provide assistance and training to developing countries to improve cybsecurity and ICT use NORM for: promote cooperation in training to develop ICT/cybersecurity awareness and skills
41:1	2018 - China, Germany hold 2nd high-level security dialogue - Xinhua _ English.news.cn	2018	The two sides stressed the importance of international cooperation and dialogue on security issues, and agreed to uphold the principle of equality, mutual trust, sincerity and being practical in further deepening their security cooperation	INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information
42:1	2018 - EU-U.S. Cyber Dialogue Joint Elements Statement - United States Department of State	2018	reaffirmed their strong partnership in favour of a global, open, stable and secure cyberspace where the rule of law fully applies	NORM for: promote an open, secure, stable, accessible, and peaceful cyber space / ICT environment
42:2	2018 - EU-U.S. Cyber Dialogue Joint Elements Statement - United States Department of State	2018	rights that individuals have offline are protected online	INDIVIDUAL RIGHTS for: acknowledging that the same rights that individuals have offline are also protected online
42:3	2018 - EU-U.S. Cyber Dialogue Joint Elements Statement - United States Department of State	2018	Both sides welcomed progress made to increase global capabilities to protect against, detect, deter, and respond to malicious cyber activities and underlined the need for coordination and cooperation in order to safeguard a global, open, stable, and secure cyberspace.	CAPACITY BUILDING CBM: encourage further work in capacity-building CYBER ATTACKS for: strengthen tools and resources needed to prepare, deter, defend, and respond to unlawful use of ICTs, cyber attacks / acts of cyber crime and/or terrorism CYBER STABILITY for: deterring cyber incidents / attacks
42:4	2018 - EU-U.S. Cyber Dialogue Joint Elements Statement - United States Department of State	2018	human rights and fundamental freedoms online and condemned undue restrictions on freedom of expression and censorship in violation of international human rights law	HUMAN RIGHTS for: applicability of international human rights law(s) to cyberspace HUMAN RIGHTS for: respecting human rights and fundamental freedoms; applying them to cyber space / ICT use, etc.
42:5	2018 - EU-U.S. Cyber Dialogue Joint Elements Statement - United States Department of State	2018	also reaffirmed their strong support for the multi-stakeholder approach to Internet governance and encourage all stakeholders to strengthen existing Internet governance mechanisms, including the Internet Governance Forum as the premier multi-stakeholder venue for dialogue on Internet-related public policy issues.	STAKEHOLDER COOPERATION for: coordinate/cooperate in preserving multistakeholder internet governance
42:6	2018 - EU-U.S. Cyber Dialogue Joint Elements Statement - United States Department of State	2018	The EU and United States also underlined the need to address the digital divide to enable economic growth, social development, and increasing cyber resilience towards cyber threats and stressed their commitment to continued capacity building assistance to this end, including through the Global Forum for Cyber Expertise	CAPACITY BUILDING CBM: encourage further work in capacity-building NORM for: supporting a free and secure internet / cyber space that supports economic growth and innovation
42:7	2018 - EU-U.S. Cyber Dialogue Joint Elements Statement - United States Department of State	2018	The EU and United States endorsed the work to date by the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UNGGE), including its landmark 2013 and 2015 reports, a	UNITED NATIONS for: following the United Nation's (UN) [2015 and or 2013] GGE report's call for all States to be guided in their use of ICTs in relation to the report
42:8	2018 - EU-U.S. Cyber Dialogue Joint Elements Statement - United States Department of State	2018	The EU and United States reaffirmed their adherence to certain voluntary, non-binding norms of responsible State behaviour in cyberspace during peacetime	STATE RESPONSIBILITY for: states should behave responsibly in cyberspace (and use ICTs responsibly) during peacetime
42:9	2018 - EU-U.S. Cyber Dialogue Joint Elements Statement - United States Department of State	2018	In addition, both sides welcomed important, ongoing work and progress on the development and implementation of cyber confidence building measures to reduce misperceptions and the risk of escalation stemming from the use of information and communications technologies	CONFIDENCE BUILDING for: CBMs' value in increasing transparency, predictability, and stability CONFIDENCE BUILDING for: develop and implement [practical] cyber confidence building measures (CBMs) between nation states STATE RESPONSIBILITY CBM: transnational consulting to reduce risk of misperception, escalation, and conflict
42:10	2018 - EU-U.S. Cyber Dialogue Joint Elements Statement - United States Department of State	2018	The EU and United States reaffirmed the importance of the Budapest Convention as a basis for national legislation and international cooperation in fighting cybercrime.	CONFIDENCE BUILDING CBM: adopt legislative basis for combatting cybercrime (i.e., the Budapest Convention) STATE RESPONSIBILITY for: adhering to rules and regulations agreed upon by previously enacted international law/mandates/treaties

ID	Document	Document Groups	Quotation Content	Codes
42:11	2018 - EU-U.S. Cyber Dialogue Joint Elements Statement - United States Department of State	2018	the EU and United States are committed to hold States accountable for actions that are contrary to the growing consensus on responsible state behaviour in cyberspace	STATE RESPONSIBILITY AND SOVEREIGNTY CBM: hold other nation states / entities accountable for actions that may be contrary to the international consensus on responsible State behavior in cyberspace
43:1	2018 - buenos_aires_leaders_declaration_0	2018	bridge the digital gender divide and further digital inclusion	DIGITAL EQUALITY CBM: work towards digital equality and inclusion (i.e., for women and traditionally marginalised groups) - this includes cooperation between the private sector, civil society, and national governments (as well as multilateral banks, and international entities such as the United Nations)
43:2	2018 - buenos_aires_leaders_declaration_0	2018	support consumer protection,	EDUCATE AND STRENGTHEN THE GENERAL PUBLIC for: providing users/customers/the general public with information and tools that will enable them to understand current and future threats, as well as protect against them
43:3	2018 - buenos_aires_leaders_declaration_0	2018	We reaffirm the importance of addressing issues of security in the use of ICTs.	CONFIDENCE BUILDING CBM: address issues [related to cyber space/cybersecurity/ICTs]
43:4	2018 - buenos_aires_leaders_declaration_0	2018	We support the free flow of information, ideas and knowledge,	INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information
43:5	2018 - buenos_aires_leaders_declaration_0	2018	intellectual property rights protection.	CYBER ATTACK for: preventing ICT-enabled theft of intellectual property (this includes trade secrets and other confidential business information)
43:6	2018 - buenos_aires_leaders_declaration_0	2018	We welcome the G20 Repository of Digital Policies to share and promote the adoption of innovative digital economy business models.	STATE RESPONSIBILITY for: adhering to rules and regulations agreed upon by previously enacted international law/mandates/treaties
43:7	2018 - buenos_aires_leaders_declaration_0	2018	We recognize the importance of the interface between trade and the digital economy.	DIGITAL ECONOMY CBM: recognize the importance of the relationship between trade and the digital economy
44:1	2018 - The Charlevoix G7 Summit Communique - Consilium	2018	addressing in particular non-market oriented policies and practices, and inadequate protection of intellectual property rights, such as forced technology transfer or cyber-enabled theft.	CYBER ATTACK for: preventing ICT-enabled theft of intellectual property (this includes trade secrets and other confidential business information)
44:2	2018 - The Charlevoix G7 Summit Communique - Consilium	2018	future where individuals' human rights are equally protected both ofine and online; and where everyone has equal opportunity to participate in political, social, economic and cultural endeavors.	DIGITAL EQUALITY CBM: work towards digital equality and inclusion (i.e., for women and traditionally marginalised groups) - this includes cooperation between the private sector, civil society, and national governments (as well as multilateral banks, and international entities such as the United Nations) HUMAN RIGHTS for: applicability of international human rights law(s) to cyberspace HUMAN RIGHTS for: respecting human rights and fundamental freedoms; applying them to cyber space / ICT use, etc. INDIVIDUAL RIGHTS for: acknowledging that the same rights that individuals have offline are also protected online
44:3	2018 - The Charlevoix G7 Summit Communique - Consilium	2018	We are committed to addressing the use of the internet for terrorist purposes, including as a tool for recruitment, training, propaganda and fnancing, and by working with partners such as the Global Internet Forum to 10/7/2020 The Charlevoix G7 Summit Communique - Consilium https://www.consilium.europa.eu/en/press/press-releases/2018/06/09/the-charlevoix-g7-summit-communique/ 5/9 Counter Terrorism.	CYBER ATTACKS for: strengthen tools and resources needed to prepare, deter, defend, and respond to unlawful use of ICTs, cyber attacks / acts of cyber crime and/or terrorism
45:1	2018 - DEC1 Declaracion Fortaleciendo CICTE01221 E (2)	2018	Their commitment to developing and/or strengthening partnerships with the private sector, civil society, and other actors to encourage the use of information and communication technologies (ICTs), including the Internet, particularly by youth, to prevent and counter violent extremism and to strengthen the development of capacities to resist and counter radicalization to violence and violent extremist propaganda directed primarily at youth.	CYBER ATTACKS for: strengthen tools and resources needed to prepare, deter, defend, and respond to unlawful use of ICTs, cyber attacks / acts of cyber crime and/or terrorism STAKEHOLDER COOPERATION for: work / intensify cooperation against criminal/terrorist use of ICTs

ID	Document	Document Groups	Quotation Content	Codes
46:1	2018 - Japan-Estonia Summit Meeting _ Ministry of Foreign Affairs of Japan	2018	continue to advance cooperation in this area, utilizing opportunities such as the Japan-Estonia Cyber Dialogue	INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information STATE RESPONSIBILITY for: adhering to rules and regulations agreed upon by previously enacted international law/mandates/treaties
47:1	2018 - NATO - Brussels Summit Declaration 11-12 July 2018, 11-Jul.-2018	2018	We reaÞrm our commitment to act in accordance with international law, including the UN Charter, international humanitarian law, and human rights law, as applicable	HUMAN RIGHTS for: applicability of international human rights law(s) to cyberspace HUMAN RIGHTS for: respecting human rights and fundamental freedoms; applying them to cyber space / ICT use, etc. INTERNATIONAL LAW for: applicability of international law to cyberspace STATE RESPONSIBILITY for: adhering to rules and regulations agreed upon by previously enacted international law/mandates/treaties
47:2	2018 - NATO - Brussels Summit Declaration 11-12 July 2018, 11-Jul.-2018	2018	We also support work to maintain international peace and security in cyberspace and to promote stability and reduce the risk of conÖict, recognising that we all stand to beneÕt from a norms-based, predictable, and secure cyberspace.	NORM for: promote an open, secure, stable, accessible, and peaceful cyber space / ICT environment NORMS CBM: further dialogue regarding norms pertaining to State use of ICTs NORMS CBM: universally agreed upon [voluntary] norms/rules/principles are important for the responsible behavior of States' use of ICTs
47:3	2018 - NATO - Brussels Summit Declaration 11-12 July 2018, 11-Jul.-2018	2018	We will establish a Cyberspace Operations Centre in Belgium to provide situational awareness and coordination of NATO operational activity within cyberspace,	INFORMATION EXCHANGE for: increasing international cooperation is required to address cyber security risks STAKEHOLDER COOPERATION for: support other international and/or regional cooperative partnerships
47:4	2018 - NATO - Brussels Summit Declaration 11-12 July 2018, 11-Jul.-2018	2018	We look forward to building on the successful implementation of our Defence and Related Security Capacity Building (DCB) assistance to Jordan in such priority areas as cyber defence	CAPACITY BUILDING CBM: encourage further work in capacity-building
48:1	2018 - Organization for Security and Cooperation (OSCE) in Europe , Ministerial Council	2018	We are committed to ensure the greatest possible access to the Internet and its benefits. Digitalization and an open, secure, reliable, interoperable and truly global Internet are enablers for inclusive economic growth	NORM for: promote an open, secure, stable, accessible, and peaceful cyber space / ICT environment NORM for: supporting a free and secure internet / cyber space that supports economic growth and innovation
48:3	2018 - Organization for Security and Cooperation (OSCE) in Europe , Ministerial Council	2018	We recognize that the free flow of and access to information, including on the Internet, are essential for the digital economy and beneficial to development.	ACCESS CBM: creating a free flow of and acccess to the internet is essential for the digital economy, and beneficial to development
48:5	2018 - Organization for Security and Cooperation (OSCE) in Europe , Ministerial Council	2018	Fostering competition in the digital economy;	DIGITAL ECONOMY for: fostering safe and secure competition in the digital economy
48:6	2018 - Organization for Security and Cooperation (OSCE) in Europe , Ministerial Council	2018	Bridging the digital divides, including through collaboration between higher education institutions;	EDUCATION for: include cybersecurity courses in school curricula (i.e., primary school, degree courses in undergrad, professional education, and trainings
48:7	2018 - Organization for Security and Cooperation (OSCE) in Europe , Ministerial Council	2018	Upholding the rule of law and protecting human rights;	HUMAN RIGHTS for: applicability of international human rights law(s) to cyberspace HUMAN RIGHTS for: respecting human rights and fundamental freedoms; applying them to cyber space / ICT use, etc. INTERNATIONAL LAW for: applicability of international law to cyberspace
48:9	2018 - Organization for Security and Cooperation (OSCE) in Europe , Ministerial Council	2018	Exchanging experiences on digital transformation, digitalisation of government and innovative models.	INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information
48:10	2018 - Organization for Security and Cooperation (OSCE) in Europe , Ministerial Council	2018	We recognize that e-government and good governance play a crucial role in modernizing and increasing efficiency in public administration and contribute to the promotion of better policy-making, transparency, integrity, accountability and the prevention of corruption.	CONFIDENCE BUILDING CBM: voluntary transparency

ID	Document	Document Groups	Quotation Content	Codes
48:11	2018 - Organization for Security and Cooperation (OSCE) in Europe , Ministerial Council	2018	We welcome the decision of the incoming 2019 Slovak OSCE Chairmanship to continue the discussions initiated by the 2018 Italian OSCE Chairmanship on the topic of digital transformation. We encourage future OSCE Chairmanships to continue these discussions on the impact of the ongoing digital transformation on our economies and societies and therefore on our common security	STAKEHOLDER COOPERATION for: support other international and/or regional cooperative partnerships
49:1	2018 - Key Takeaways from the Singapore International Cyber Week - Access Partnership	2018	The ASEAN Ministerial Conference on Cybersecurity (AMCC) participants subscribed to 11 of the voluntary, non-binding norms recommended in the Report of the United Nations Group of Governmental Experts (UNGGE) back in 2015, demonstrating the region's strong commitment to creating a more stable and secure cybersecurity framework and promoting socio-economic development.	UNITED NATIONS for: following the United Nation's (UN) [2015 and or 2013] GGE report's call for all States to be guided in their use of ICTs in relation to the report
49:2	2018 - Key Takeaways from the Singapore International Cyber Week - Access Partnership	2018	Singapore announced a SGD 30 million (USD 22 million) investment into the ASEAN-Singapore Cybersecurity Centre for Excellence (ASCCE) to respond to the current gap in the talent pool in the cybersecurity industry. The ASCCE will serve as a Cyber Think-Tank and Training Centre, a Computer Emergency Response Team (CERT) Centre, and a Cyber Range Training Centre	CAPACITY BUILDING CBM: pioritize ICT security awareness and capacity-building in national plans and budgets EMERGENCY RESPONSE CBM: each state/regional partnership should establish and/or strengthen a national computer emergency response team (CERT) / cybersecurity incident response team
49:3	2018 - Key Takeaways from the Singapore International Cyber Week - Access Partnership	2018	Simultaneously, the Cybersecurity Agency of Singapore (CSA) announced the creation of the Singapore-UN Cyber Programme in partnership with the United Nations Ofce for Disarmament Afairs (UNODA). The organisations will conduct an annual Norms Awareness Workshop and Cyber Policy Scenario Planning Workshop for representatives from the ASEAN member states. On a related note, the UNODA have developed a norms implementation toolkit with model policies, lessons, and resources	NORM for: promote cooperation in training to develop ICT/cybersecurity awareness and skills NORMS for: promote awareness of existing and/or proposed norms, as well as support their operationalization
49:4	2018 - Key Takeaways from the Singapore International Cyber Week - Access Partnership	2018	greater multistakeholder engagement on the issue of cybersecurity.	STAKEHOLDER COOPERATION for: establishing a standing multistakeholder engagement mechanism in order to address stability issues (this includes adequate involvement and consultation of states, non-state actors such as private sector entities, and civil society)
49:5	2018 - Key Takeaways from the Singapore International Cyber Week - Access Partnership	2018	Bounty programme calling for both international and local white-hat hackers to test selected, Internet-facing government systems and identify vulnerabilities.	PRODUCT CBM: transparency and dialogue regarding ICT vulnerabilities and identified harmful hidden functions in ICT products
50:1	2018 - Japan-US-ROK Experts Meeting on Cybersecurity _ Ministry of Foreign Affairs of Japan	2018	promoting an open, interoperable, reliable, and secure Internet	NORM for: promote an open, secure, stable, accessible, and peaceful cyber space / ICT environment
50:2	2018 - Japan-US-ROK Experts Meeting on Cybersecurity _ Ministry of Foreign Affairs of Japan	2018	trilateral cooperation to enhance international cyber stability, deter malicious activities in cyberspace, and counter cyber threats, including from state actors	CYBER STABILITY for: deterring cyber incidents / attacks STAKEHOLDER COOPERATION CBM: states should participate and cooperate in multilateral forums
50:3	2018 - Japan-US-ROK Experts Meeting on Cybersecurity _ Ministry of Foreign Affairs of Japan	2018	Participants also discussed cybersecurity of the 2018 and 2020 Olympics and Paralympic Games, capacity building efforts, and regional cyber policy coordination	CAPACITY BUILDING CBM: encourage further work in capacity-building CONFIDENCE BUILDING for: promote cooperation in regional confidence-building measures (CBMs)
50:4	2018 - Japan-US-ROK Experts Meeting on Cybersecurity _ Ministry of Foreign Affairs of Japan	2018	the Japan-US-ROK trilateral experts meeting on cybersecurity was held in Washington D.C. 2. Mr. Masaki Yasumatsu, Director of the Cyber Policy Division, Foreign Policy Bureau, Ministry of Foreign Affairs, led the delegation from Japan. He was accompanied by representatives from the National Center of Incident Readiness and Strategy for Cybersecurity (NISC), the National Police Agency (NPA), the Cabinet Intelligence and Research Office (CIRO), the Public Security Intelligence Agency (PSIA), the Ministry of Internal Affairs and Communications (MIC), the Ministry of Foreign Affairs (MOFA), the Ministry of Economy, Trade, and Industry (METI), the Ministry of Defense (MOD), the Japan Computer Emergency Response Team Cordination Center (JPCERT/CC), and the Information-technology Promotion Agency, Japan (IPA)	INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information
51:1	2018 - JointUS–UK+Statement_4-16-2018	2018	Today, the U.S. Department of Homeland Security (DHS), Federal Bureau of Investigation (FBI), and the UK's National Cyber Security Centre (NCSC) released a joint Technical Alert about malicious cyber activity carried out by the Russian Government	INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information

ID	Document	Document Groups	Quotation Content	Codes
51:3	2018 - JointUS–UK+Statement_4-16-2018	2018	We condemn this latest activity in the strongest possible terms and we will not accept nor tolerate any malign foreign cyber operations, intrusions, or compromises —to include inÂuence operations	CYBER ATTACKS against: conducting ICT operations intended to disrupt essential infrastructure of political processes (i.e., election processes)
51:4	2018 - JointUS–UK+Statement_4-16-2018	2018	We call on all responsible nations to use their resources—including diplomatic, law enforcement, technical, and other means—to address the Russian cyber threat.	STATE RESPONSIBILITY AND SOVEREIGNTY CBM: hold other nation states / entities accountable for actions that may be contrary to the international consensus on responsible State behavior in cyberspace
51:5	2018 - JointUS–UK+Statement_4-16-2018	2018	“Cyber security is a shared responsibility, and we understand that identifying a threat in one organisation’s network can prevent an attack in another. Today’s joint Technical Alert is an example of how we are working with allies and partners to prevent cyber actors from impacting critical infrastructure to the fullest extent possible.	STAKEHOLDER COOPERATION for: working with partners / sharing responsibility in identifying threats and keeping shared network's safe
52:1	2018 - A_RES_73_27_E	2018	Noting that capacity-building is essential for cooperation of States and confidence-building in the field of ICT security,	CAPACITY BUILDING CBM: encourage further work in capacity-building CYBERSPACE STABILITY for: state and non-state actors (including international entities) should increase efforts to build capacity and capabilities (i.e., train staff) and promote a shared understanding of the importance of the stability of cyberspace
52:3	2018 - A_RES_73_27_E	2018	Stressing that it is in the interest of all States to promote the use of ICTs for peaceful purposes, with the objective of shaping a community of shared future for humankind in cyberspace, and that States also have an interest in preventing conflict arising from the use of ICTs,	CONFIDENCE BUILDING CBM: promote the use of ICTs for peaceful purposes
52:4	2018 - A_RES_73_27_E	2018	Noting that the United Nations should play a leading role in promoting dialogue among Member States to develop common understandings on the security of and the use of ICTs, as well as in developing common understandings on the application of international law and norms, rules and principles for responsible State behaviour in this sphere, encourage regional efforts, promote confidence-building and transparency measures and support capacity-building and the dissemination of best practices	UNITED NATIONS CBM: the United Nations (UN) may serve as an international body for decision-making, framework creation/implementation, and when developing and adopting universally agreed upon ICT norms/rules/principles (in order to ensure peace and responsible behavior/ICT use)
52:5	2018 - A_RES_73_27_E	2018	Expressing concern that embedding harmful hidden functions in ICTs could be used in ways that would affect secure and reliable ICT use and the ICT supply chain for products and services, erode trust in commerce and damage national security,	DIGITAL ECONOMY for: further ensuring the integrity of the ICT supply chain
52:6	2018 - A_RES_73_27_E	2018	Underlining the importance of respect for human rights and fundamental freedoms in the use of ICTs	HUMAN RIGHTS for: applicability of international human rights law(s) to cyberspace HUMAN RIGHTS for: respecting human rights and fundamental freedoms; applying them to cyber space / ICT use, etc.
52:7	2018 - A_RES_73_27_E	2018	Welcoming also that, in considering the application of international law to State use of ICTs, the Group of Governmental Experts, in its 2015 report	UNITED NATIONS for: following the United Nation's (UN) [2015 and or 2013] GGE report's call for all States to be guided in their use of ICTs in relation to the report
52:9	2018 - A_RES_73_27_E	2018	Charter of the United Nations and other international law	INTERNATIONAL LAW for: applicability of international law to cyberspace STATE RESPONSIBILITY for: adhering to rules and regulations agreed upon by previously enacted international law/mandates/treaties
52:10	2018 - A_RES_73_27_E	2018	the settlement of international disputes by peaceful means in such a manner that international peace and security and justice are not endangered	STATE RESPONSIBILITY for: settling disputes (international and/or domestic) through peaceful means, in order to not endanger peace, security, and justice
52:12	2018 - A_RES_73_27_E	2018	that voluntary and non-binding norms, rules and principles of responsible behaviour of States in the use of ICTs can reduce risks to international peace, security and stability	NORMS CBM: universally agreed upon [voluntary] norms/rules/principles are important for the responsible behavior of States' use of ICTs
52:13	2018 - A_RES_73_27_E	2018	given the unique attributes of such technologies, additional norms can be developed over time,	NORMS for: continue to create and improve upon existing norms
52:15	2018 - A_RES_73_27_E	2018	Reaffirming the right and duty of States to combat, within their constitutional prerogatives, the dissemination of false or distorted news, which can be interpreted as interference in the internal affairs of other States or as being harmful to the promotion of peace, cooperation and friendly relations among States and nations	STATE RESPONSIBILITY for: establishing a framework / procedures to combat the 'fake news' (maliciously produced false information) phenomenon
52:16	2018 - A_RES_73_27_E	2018	Recognizing the duty of a State to abstain from any defamatory campaign, vilification or hostile propaganda for the purpose of intervening or interfering in the internal affairs of other States,	STATE SOVEREIGNTY for: state sovereignty applied to State's ICT activities & ICT infrastructure within their territory

ID	Document	Document Groups	Quotation Content	Codes
52:17	2018 - A_RES_73_27_E	2018	However, the indication that an ICT activity was launched or otherwise originates from the territory or objects of the ICT infrastructure of a State may be insufficient in itself to attribute the activity to that State. Accusations of organizing and implementing wrongful acts brought against States should be substantiated. 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.	STATE SOVEREIGNTY disagreement: finding States at fault for internationally recognized wrongful ICT acts committed by on state territory
52:18	2018 - A_RES_73_27_E	2018	States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs. 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	CYBER ATTACKS against: using proxies for [international] wrongful cyber acts STATE RESPONSIBILITY & SOVEREIGNTY against: allowing non-State actors in their territories to unlawfully use ICT STATE RESPONSIBILITY & SOVEREIGNTY for: ensuring that one's territory is not used by non-State actors to commit internationally wrongful acts using ICTs
52:19	2018 - A_RES_73_27_E	2018	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.	INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information
52:21	2018 - A_RES_73_27_E	2018	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 publi	CRITICAL INFRASTRUCTURE against: knowingly damaging critical infrastructure CRITICAL INFRASTRUCTURE against: knowingly support cyberactivity that intentionally damages or impairs the use and operation of critical infrastructure
52:22	2018 - A_RES_73_27_E	2018	States should take appropriate measures to protect their critical infrastructure from ICT threats, taking into account General Assembly resolution 58/199 of 23 December 2003 on the creation of a global culture of cybersecurity and the protection of critical information infrastructures, and other relevant resolutions.	CRITICAL INFRASTRUCTURE for: promoting resilience (as related to ICTs,cybersecurity, and related critical infrastructure CRITICAL INFRASTRUCTURE for: protecting critical infrastructures
52:23	2018 - A_RES_73_27_E	2018	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.	CYBER ATTACKS for: responding to requests for help in the event of a cyber attack
52:24	2018 - A_RES_73_27_E	2018	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.	DIGITAL ECONOMY for: further ensuring the integrity of the ICT supply chain
52:25	2018 - A_RES_73_27_E	2018	States should seek to prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions.	PRODUCT TAMPERING against: states and non-state actors tampering with products/services (knowingly inserting harmful material into their products) NOR allowing their products to be tampered with TAMPERING for: adopt practices that reduce the risk of tampering as well as permit response if tampering is discovered
52:26	2018 - A_RES_73_27_E	2018	States should encourage responsible reporting of ICT vulnerabilities and share associated information on available remedies for such vulnerabilities to limit and possibly eliminate potential threats to ICTs and ICT-dependent infrastructure	PRODUCT CBM: transparency and dialogue regarding ICT vulnerabilities and identified harmful hidden functions in ICT products PRODUCT for: creating transparent procedures and frameworks to asses whether and when to disclose not publicly known vulnerabilities or flaws in their information systems and/or technologies PRODUCT for: developers and producers of products and services should take measures to timely mitigate vulnerabilities that are later discovered and be transparent about their process
52:27	2018 - A_RES_73_27_E	2018	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	CYBER ATTACKS against: targeting emergency response teams
52:28	2018 - A_RES_73_27_E	2018	A State should not use authorized emergency response teams to engage in malicious international activity.	CYBER ATTACKS against: states using authorized emergency response teams to engage in malicuous / harmful international activity

ID	Document	Document Groups	Quotation Content	Codes
52:29	2018 - A_RES_73_27_E	2018	States should encourage the private sector and civil society to play an appropriate role to improve security of and in the use of ICTs, including supply chain security for ICT products and services. States should cooperate with the private sector and the organizations of civil society in the sphere of implementation of rules of responsible behaviour in information space with regard to their potential role;	STAKEHOLDER COOPERATION for: encourage participation of other stakeholders such as the private sector, academia, and civil society orgs (as appropriate) for CBM and/or norm creation and implementation STAKEHOLDER COOPERATION for: work with states and/or the private sector/civil society (international and/or domestic) to further cooperate on topics such as law enforcement, prosecution, investment, e-commerce, intellectual property rights, etc.
53:1	2017 - igf2017_-_12th_igf_chairs_summary	2017	There was broad support for the notion that as the Internet and digital technologies continue to evolve, better coordinated digital governance systems are needed to maximise the opportunities offered by these technologies, and address the challenges they bring	CAPACITY BUILDING for: the internet and digital technologies must continue to evolve DIGITAL GOVERNANCE for: better coordinated digital governance systems are needed to maximise the opportunities offered by evolving technologies, as well as address the issues that they bring
53:2	2017 - igf2017_-_12th_igf_chairs_summary	2017	That effective digital governance adapts and responds to the needs of the global citizens, was shared by all participant	DIGITAL GOVERNANCE for: digital governance must adapt and respond to the needs of citizens
53:3	2017 - igf2017_-_12th_igf_chairs_summary	2017	Others stressed that governance structures need to focus on enhancing confidence and trust in digital technologies, ensuring security, and creating stability and predictability in cyberspace.	DIGITAL GOVERNANCE for: digital governance structures need to focus on enhancing confidence and trust in digital technologies, ensuring security and creating stability and predictability in cyberspace
53:4	2017 - igf2017_-_12th_igf_chairs_summary	2017	The notion that the ideal future digital global governance should be value-based, inclusive, open, and transparent gained traction along the debate	DIGITAL GOVERNANCE for: future digital [global] governance should be value-based, inclusive, open, and transparent
53:6	2017 - igf2017_-_12th_igf_chairs_summary	2017	It was underlined that the challenges of the digital world also need to be addressed by governments and intergovernmental organisations, through laws and regulation	STAKEHOLDER COOPERATION for: governments and intergovernmental orgs should address the challenges of the digital world through laws and regulations
53:7	2017 - igf2017_-_12th_igf_chairs_summary	2017	On the suitability of an international treaty or convention to address challenges such as cybercrime and cybersecurity, some expressed the view that it might be too early to consider such an option – without excluding it as an option for the future - while others considered that an intergovernmental treaty is not an adequate solution to tackle challenges that affect all stakeholders, and for which all stakeholders should have roles and responsibilities	STATE RESPONSIBILITY disagreement: international treaties/conventions useful in addressing challenges such as cybercrime and cybersecurity
53:8	2017 - igf2017_-_12th_igf_chairs_summary	2017	The IGF, as a multistakeholder and inclusive process, was broadly supported as an important platform that allows stakeholders to reflect critically on existing digital governance processes, and contribute to the shaping of future processes.	STAKEHOLDER COOPERATION for: establishing a standing multistakeholder engagement mechanism in order to address stability issues (this includes adequate involvement and consultation of states, non-state actors such as private sector entities, and civil society)
53:9	2017 - igf2017_-_12th_igf_chairs_summary	2017	It is important to have a process in place that ensures: transparency, adequate oversight, and redress mechanisms.	EMERGENCY RESPONSE for: creating and implementing a process that ensures transparency, adequate oversight, and redressing mechanisms when dealing with an internet shutdown of any kind
53:10	2017 - igf2017_-_12th_igf_chairs_summary	2017	Tools developed or employed to undermine encryption can come into the hands of those with illegal or criminal purposes. Governments and industry should cooperate and identify vulnerabilities in encryption/encrypted products and should be reported to the vendors	PRODUCT for: developers must strive to create secure products for society; such products will require consistent updates and improvements upon security; products must work as developers claim they will (i.e., confidentiality based encryption/data-storage/transmission) PRODUCT for: governments and private sector should cooperate in identifying vulnerabilities within encryption/encrypted products (and then notify developers/vendors of these issues)
53:11	2017 - igf2017_-_12th_igf_chairs_summary	2017	Stakeholders should work together on achieving an appropriate balance between the interests of citizens and entities to secure their data and the needs of law enforcement agencies, while not undermining the fundamentals of the technology	STAKEHOLDER COOPERATION for: stakeholders working together on achieving an appropriate balance between the interests of citizens/entities to secure their data, and the needs of law enforcement agencies (while not undermining the fundamentals of technology)
53:12	2017 - igf2017_-_12th_igf_chairs_summary	2017	As governments and private companies collect and process large amounts of data, there is a need for more transparency and accountability in these processes. Users should be educated on how their data may be used and how to protect it.	DIGITAL GOVERNANCE for: transparency and accountability when governments and/or private companies collect and process large amounts of data EDUCATION for: educating users/customers on how their data may be used, and how to protect it
53:13	2017 - igf2017_-_12th_igf_chairs_summary	2017	Governments, private companies, and civil society should work together on basic sets of rules that allow data aggregation and data flows, while also protecting the integrity of data and the privacy of individuals.	ACCESS CBM: creating a free flow of and acccess to the internet is essential for the digital economy, and beneficial to development CONFIDENCE BUILDING for: ensuring the free flow of data while also protecting the integrity of that data and the privacy of individual users

ID	Document	Document Groups	Quotation Content	Codes
53:14	2017 - igf2017_-_12th_igf_chairs_summary	2017	There was broad support for the idea that we should avoid over- focusing on the risks, and rather put emphasis on maximising the positive aspects of digitisation	CYBERSPACE STABILITY for: avoid over-fousing on the risks of digitization - and instead, put emphasis on maximising the positive aspects of said digitization
53:15	2017 - igf2017_-_12th_igf_chairs_summary	2017	Many emphasised that core principles – such as accountability, transparency, legitimacy, and openness – are needed to consolidate or restore trust. Digital technologies can help put these principles into practice	CONFIDENCE BUILDING CBM: voluntary transparency STATE RESPONSIBILITY for: enacting cybersecurity measures that will protect people (privacy, and physical safety, etc) and inform users (transparency)
53:16	2017 - igf2017_-_12th_igf_chairs_summary	2017	Some noted that governments are mainly responsible, and should invest in education and media literacy, instead of building new institutions and policies. Governments were called upon to abstain from content regulation and censorship. Some were in favour of intermediary responsibility and the need for regulation in this regard, while others argued that platforms cannot be solely responsible for countering misinformation.	STATE RESPONSIBILITY disagreement: who should be responsible for combatting fake news? (governments, intermediaries, or the platforms disseminating the information?) STATE RESPONSIBILITY for: establishing a framework / procedures to combat the 'fake news' (maliciously produced false information) phenomenon
53:17	2017 - igf2017_-_12th_igf_chairs_summary	2017	While acknowledging the importance of education, several other remedies were proposed for addressing the challenges of misinformation in the digital space: strengthening quality journalism, rebalancing the relation between traditional and new media, fact checking, and providing alternative positive stories.	STATE RESPONSIBILITY CBM: combatting disinformation/misinformation/fake news (i.e., through education, quality journalism, rebalancing the relationship between traditional and new media, fact checking, and providing alternative [positive] stories)
53:18	2017 - igf2017_-_12th_igf_chairs_summary	2017	Hence, a global culture of cybersecurity is needed, to enhance mutual understanding among stakeholders on what, when, how can be done to ensure an open, secure, stable, and accessible cyberspace	CONFIDENCE BUILDING for: agreeing on a global definition for cybersecurity and related culture
53:19	2017 - igf2017_-_12th_igf_chairs_summary	2017	While there is broad agreement that international law applies to cyberspace, calls were made for more efforts to clarify how it applies, and to identify whether there are areas where there might be gaps that international law does not cover.	INTERNATIONAL LAW for: applicability of international law to cyberspace INTERNATIONAL LAW for: identifying gaps (if any) when applying international law to cyberspace
53:20	2017 - igf2017_-_12th_igf_chairs_summary	2017	Avoiding the militarisation of cyberspace and ensuring that states do not engage in a cyber arms race were seen as important elements in this regard. For some, this can best be achieved through international cooperation among states, in the framework of the UN	CYBER STABILITY for: avoiding militarization and arms races in cyberspace UNITED NATIONS CBM: the United Nations (UN) may serve as an international body for decision-making, framework creation/implementation, and when developing and adopting universally agreed upon ICT norms/rules/principles (in order to ensure peace and responsible behavior/ICT use)
53:21	2017 - igf2017_-_12th_igf_chairs_summary	2017	Calls were made for more awareness raising about these norms, and more efforts to enhance their voluntary implementation.	NORMS for: continue to create and improve upon existing norms NORMS for: promote awareness of existing and/or proposed norms, as well as support their operationalization
53:22	2017 - igf2017_-_12th_igf_chairs_summary	2017	Moreover, if a treaty is adopted, the question remains on how to make sure that it is actually implemented, considering that it is not even clear how existing international law applies to the use of digital technologies by states.	INTERNATIONAL LAW disagreement: how to implement/enfoce a treaty regarding norms/rules/principles (considering that there is uncertainty about how international law applies to cyberspace)
53:23	2017 - igf2017_-_12th_igf_chairs_summary	2017	Community networks are an example of such a multidisciplinary approach: the building of physical infrastructures is complemented by empowering communities to benefit from digital opportunities. Public libraries also have an important role to play in improving access, especially in developing countries.	DIGITAL EQUALITY for: closing the digital divide (i.e., by empowering communities to benefit from digital opportunities)
53:24	2017 - igf2017_-_12th_igf_chairs_summary	2017	Measures are implemented around the world, and it is important to collect data about what works and what does not, to inform policy making.	ACCESS for: collect data on the measures that work and don't work regarding universal design in the development of technologies in order to enhance accessibility
53:25	2017 - igf2017_-_12th_igf_chairs_summary	2017	Beyond these values, human rights need to be protected online. For example, privacy and data protection rights remain a major concern, and principles such as privacy-by- design and consent-by-design could contribute to better preserving them. Children and gender rights are also important, and their implementation requires both digital literacy and protection from online harm and violence.	HUMAN RIGHTS CBM: domestic and international cooperation amongst nation states, private sector, civil society, and other non-government entities is important in order to strengthen human rights in cyber space / ICT use, etc. HUMAN RIGHTS for: applicability of international human rights law(s) to cyberspace HUMAN RIGHTS for: respecting human rights and fundamental freedoms; applying them to cyber space / ICT use, etc.
53:26	2017 - igf2017_-_12th_igf_chairs_summary	2017	As technologies continue to develop, new challenges need to be addressed	CONFIDENCE BUILDING for: addressing new challenges as technologies continue to develop/evolve

ID	Document	Document Groups	Quotation Content	Codes
53:27	2017 - igf2017_-_12th_igf_chairs_summary	2017	There was broad support for the view that the rights - people have offline should also be protected online.	INDIVIDUAL RIGHTS for: acknowledging that the same rights that individuals have offline are also protected online
53:28	2017 - igf2017_-_12th_igf_chairs_summary	2017	It was generally supported that access to the Internet is an important enabler of development and growth	ACCESS CBM: access to the internet is an important enabler of development./growth/innovation
53:29	2017 - igf2017_-_12th_igf_chairs_summary	2017	Many indicated that the Internet enables them to exercise their digital rights, and called for more education, digital literacy, and for raising awareness about digital rights, and ways to exercise and protect them	EDUCATION for: increased eduation, [digital] literacy, and awareness regarding digital rights and ways to exercise/protect them
53:30	2017 - igf2017_-_12th_igf_chairs_summary	2017	Some recommended that the protection of digital rights should be embedded in an inclusive approach that also considers the needs and rights of vulnerable groups and communities – such as children, women, gender minorities, people with disabilities	DIGITAL EQUALITY for: the protection of digital rights should be embedded in an inclusive approach (i.e., also considers the needs/rights of vulnerable groups such as children, women, gender minorities, people w/ disabilities, etc.)
53:31	2017 - igf2017_-_12th_igf_chairs_summary	2017	Suggested solutions to maximise the opportunities and minimise the risks included the adoption of standards and principles on issues such as security and privacy, ethics, and accountability.	ARTIFICIAL INTELLIGENCE CBM: incorporate cooperation through a multistakeholder lense in designing and applying standards and principles (such as transparency and responsibility) towards artificial intelligent systems and related technologies ARTIFICIAL INTELLIGENCE for: holding states/developers/humans responsible for artificial intelligence (AI) systems and their actions
53:32	2017 - igf2017_-_12th_igf_chairs_summary	2017	There was a broad confidence that multistakeholder processes could be effective in addressing challenges related to digital rights. It was noted that more efforts should be made to strengthen the engagement of stakeholders, and empower them to make meaningful contributions.	STAKEHOLDER COOPERATION for: coordinate/cooperate in preserving multistakeholder internet governance STAKEHOLDER COOPERATION for: encourage participation of other stakeholders such as the private sector, academia, and civil society orgs (as appropriate) for CBM and/or norm creation and implementation
53:33	2017 - igf2017_-_12th_igf_chairs_summary	2017	Efforts to enable women and girls to access the infrastructures and digital technologies need to be complemented with creating digital literacy, enabling meaningful use of technologies, encouraging them to prepare for jobs in technology fields, enabling them to create content that is relevant and valuable to their lives and contexts, as well as empowering them to contribute to Internet governance and digital policy processes	DIGITAL EQUALITY for: closing the gender digital divide (focusing on women and girls, but also those a part of gender subgroups such as the LGBTQI+ communiy)
53:34	2017 - igf2017_-_12th_igf_chairs_summary	2017	Several discussants stated that technology is not neutral, and that gender diversity should be taken into account when technologies are designed. They warned for the potential impact of data-driven technologies on gender digital rights, and called for multistakeholder action to avoid that opaque algorithms and machine learning systems make gender-biased decisions.	DIGITAL EQUALITY for: gender diversity should be taken into account when technologes are designed
53:35	2017 - igf2017_-_12th_igf_chairs_summary	2017	Some warned that states and Internet intermediaries, when tackling online gender- based abuse and violence should not do so through a protectionist framework, but through the framework of human rights. This includes the need to potentially balance different rights, and that the principles of necessity, proportionality, and transparency should be respected in so far as they limit the freedom of expression.	HUMAN RIGHTS for: addressing online gender-abuse/violence through a human rights framework
53:36	2017 - igf2017_-_12th_igf_chairs_summary	2017	The important role played by civil society actors in developing research and coordinating collaboration to understand key and emerging gender-related issues were acknowledged, and policymakers were encouraged to engage and be part of honest conversations to develop not only policies but coordinated plans together to achieve concrete results.	DIGITAL EQUALITY for: engaging policymakers in honest conversations involving gender-related issues in cyberspace STAKEHOLDER COOPERATION CBM: civil society is important when developing research, coordinating, and collaborating in understanding key and emerging gender-related issues
53:37	2017 - igf2017_-_12th_igf_chairs_summary	2017	E-commerce was seen as an enabler of global trade, empowering enterprises to reach international markets.	DIGITAL ECONOMY CBM: recognize the importance of the relationship between trade and the digital economy
53:38	2017 - igf2017_-_12th_igf_chairs_summary	2017	then also touched upon a need to update cross-border trade rules and procedures, to better cater for the digital era	DIGITAL ECONOMY disagreement: updating international trade rules and procedures to better cater for the digital era
53:39	2017 - igf2017_-_12th_igf_chairs_summary	2017	Other focused on the need to address risks associated with such technologies, from bias and imbalances in algorithmic decision making, to disruptions on the labour market and workforce	ARTIFICIAL INTELLIGENCE for: holding states/developers/humans responsible for artificial intelligence (AI) systems and their actions ARTIFICIAL INTELLIGENCE for: identify and address risks associated with artificial intelligence and related technologies
54:1	2017 - singaporenew-digital	2017	“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.”	PRODUCT TAMPERING against: states and non-state actors tampering with products/services (knowingly inserting harmful material into their products) NOR allowing their products to be tampered with

ID	Document	Document Groups	Quotation Content	Codes
54:2	2017 - singaporenew-digital	2017	“State and non-state actors should not commandeer others’ ICT resources for use as botnets or for similar purposes	CYBER ATTACKS against: comandeering the general public's ICT resources for use as botnets or for similar purposes
54:3	2017 - singaporenew-digital	2017	“States should create procedurally transparent frameworks to assess whether and when to disclose not publicly known vulnerabilities or faws they are aware of in information systems and technologies. The default presumption should be in favor of disclosure	PRODUCT for: creating transparent procedures and frameworks to asses whether and when to disclose not publicly known vulnerabilities or flaws in their information systems and/or technologies
54:4	2017 - singaporenew-digital	2017	“Developers and producers of products and services on which the stability of cyberspace depends should prioritize security and stability, take reasonable steps to ensure that their products or services are free from signifcant vulnerabilities, take measures to timely mitigate vulnerabilities that are later discovered and to be transparent about their process. All actors have a duty to share information on vulnerabilities in order to help prevent or mitigate malicious cyber activity.	CONFIDENCE BUILDING CBM: voluntary transparency PRODUCT for: developers and producers of products and services should prioritize security and stability PRODUCT for: developers and producers of products and services should take measures to timely mitigate vulnerabilities that are later discovered and be transparent about their process PRODUCT for: developers and producers of products and services should take reasonable steps to ensure that their products/services are free from significant vulnerabilities
54:5	2017 - singaporenew-digital	2017	“States should enact appropriate measures, including laws and regulations, to ensure basic cyber hygiene.	STATE RESPONSIBILITY for: nation-state enacted laws and/or regulations to ensure basic cyber protocols/cleanliness/hygiene
54:6	2017 - singaporenew-digital	2017	“Non-state actors should not engage in offensive cyber operations and state actors should prevent and respond to such activities if they occur	CYBER ATTACKS against: [non-state actors] engaging in offensive/harmful cyber operations of any kind CYBER ATTACKS for: responding to requests for help in the event of a cyber attack EMERGENCY RESPONSE for: prevent and manage a cross-border (international/transnational) cyber event from both supervisory and industry perspective STATE RESPONSIBILITY for: responding to offensive/illegal/unlawful cyber activities by non state actors if/when discovered
54:7	2017 - singaporenew-digital	2017	“Without prejudice to their rights and obligations, state and non-state actors should not conduct or 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.	CYBER STABILITY for: protecting the public core of the internet NORM against: states and non-state actors conducting activity that intentionally and substantially damages the general availability or integrity of the public core of the internet
54:8	2017 - singaporenew-digital	2017	“State and non-state actors should not pursue, support or allow cyber operations intended to disrupt the technical infrastructure essential to elections, referenda or plebiscites.”	CYBER ATTACKS against: conducting ICT operations intended to disrupt essential infrastructure of political processes (i.e., election processes)
54:9	2017 - singaporenew-digital	2017	DEFINITION OF THE PUBLIC CORE, TO WHICH THE NORM APPLIES	CONFIDENCE BUILDING for: defining the public core of the internet
55:1	2017 - MunichSecurityReport2017	2017	A ministry of defense strategy for sustained technology development should allow for an outside-in innovation process, a streamlined approach to defning requirements, and simplifed procurement of digital technologies. New forms of part- nering with emerging tech companies will also be needed.	CAPACITY BUILDING CBM: in order for sustained technological development, defense strategies should allow for an 'outside-in' innovation process (streamlining and defining requirements, and simplifying the procurement of digital technologies) STAKEHOLDER COOPERATION CBM: new forms of partnering with emerging tech companies will also be needed
56:1	2017 - 2nd-AMCC-Chairmans-Statement-cleared	2017	AMCC participants agreed that the AMCC continued to be a useful platform for facilitating discussions of cross-cutting cybersecurity issues among ICT Ministers and Cybersecurity Ministers and Senior Officials from all ASEAN Member States	STAKEHOLDER COOPERATION for: working with partners / sharing responsibility in identifying threats and keeping shared network's safe
56:2	2017 - 2nd-AMCC-Chairmans-Statement-cleared	2017	They also reaffirmed the need for ASEAN to take a holistic and more coordinated approach to regional cybersecurity cooperation and capacity building.	CAPACITY BUILDING for: taking a holistic and coordinated approach when addressing regional cybersecurity cooperation and capacity building
56:3	2017 - 2nd-AMCC-Chairmans-Statement-cleared	2017	Participants recognised that cybersecurity was an issue that required coordinated expertise from multiple stakeholders from across different domains to address effectively,	ARTIFICIAL INTELLIGENCE CBM: incorporate cooperation through a multistakeholder lense in designing and applying standards and principles (such as transparency and responsibility) towards artificial intelligent systems and related technologies STAKEHOLDER COOPERATION for: establishing a standing multistakeholder engagement mechanism in order to address stability issues (this includes adequate involvement and consultation of states, non-state actors such as private sector entities, and civil society)
56:4	2017 - 2nd-AMCC-Chairmans-Statement-cleared	2017	and the promotion of international voluntary cyber norms of responsible State behaviour was important for cultivating trust and confidence and the eventual development of a rules-based cyberspace	NORMS CBM: universally agreed upon [voluntary] norms/rules/principles are important for the responsible behavior of States' use of ICTs

ID	Document	Document Groups	Quotation Content	Codes
56:5	2017 - 2nd-AMCC-Chairmans-Statement-cleared	2017	To that end, participants underscored the importance of enhancing coordination between various platforms of the three pillars of ASEAN in addressing the cross-cutting issue of cybersecurity and to counter increasingly sophisticated cyber threats, so that ASEAN's efforts are focused, effective, and neither duplicated nor working at cross purposes with one another	INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information STATE RESPONSIBILITY for: dialogue amongst nations by an international body
56:6	2017 - 2nd-AMCC-Chairmans-Statement-cleared	2017	In this regard, participants noted the recommendations regarding norms set out in the 2015 Report of the United Nations Group of Government Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UNGGE).	UNITED NATIONS for: following the United Nation's (UN) [2015 and or 2013] GGE report's call for all States to be guided in their use of ICTs in relation to the report
56:7	2017 - 2nd-AMCC-Chairmans-Statement-cleared	2017	Participants further proposed the use of International Telecommunications Union (ITU) Global Cybersecurity Index (GCI) as a possible benchmark for assessing and developing ASEAN's cybersecurity readiness. In addition, participants noted that linkages to privacy should be considered when considering cybersecurity policy.	INFORMATION EXCHANGE for: establish a formal framework to facilitate professional dialogue STAKEHOLDER COOPERATION CBM: form bilateral and multilateral cooperation initiatives to build on established partnerships/relationships
57:1	2017- ASEAN-DECLARATION-TO-PREVENT-AND-COMBAT-CYBERCRIME	2017	importance of Information and Communications Technologies (ICTs) as the key driver of ASEAN Member States in governance, economy, commerce and trade, social well-being and all other aspects;	CONFIDENCE BUILDING CBM: recognize importance of ICTs as the key driver of governance, economy, commerce, trade, and social well-being
57:2	2017- ASEAN-DECLARATION-TO-PREVENT-AND-COMBAT-CYBERCRIME	2017	imperative to have National Action Plans in place that will contain national policies and strategies to prevent and combat cybercrime as well as the implementation of anti-cybercrime-related measures;	CONFIDENCE BUILDING CBM: adopt legislative basis for combatting cybercrime (i.e., the Budapest Convention) STATE RESPONSIBILITY CBM: recognize the imperative to have National Action Plans (NAPs) in place in order to contain national policies and strategies intended to prevent and combat cybercrime
57:3	2017- ASEAN-DECLARATION-TO-PREVENT-AND-COMBAT-CYBERCRIME	2017	need to enhance cooperation against cybercrime aimed at the protection of our community in the region including by, inter alia, formulating concrete and effective regional approaches;	STAKEHOLDER COOPERATION for: coordinate/cooperate in combatting cybercrime
57:4	2017- ASEAN-DECLARATION-TO-PREVENT-AND-COMBAT-CYBERCRIME	2017	RECALLING the ASEAN Declaration on Transnational Crime, signed by the ASEAN Ministers of Interior/Home Affairs on 20 December 1997 in Manila, Philippines, during the 1st ASEAN Ministerial Meeting on Transnational Crime (AMMTC), which agreed to strengthen the commitment of Member States to cooperate at the regional level in combating transnational crimes	STATE RESPONSIBILITY for: adhering to rules and regulations agreed upon by previously enacted international law/mandates/treaties
57:5	2017- ASEAN-DECLARATION-TO-PREVENT-AND-COMBAT-CYBERCRIME	2017	RECALLING FURTHER the ASEAN Plan of Action to Combat Transnational Crime 2016-2025, which was adopted by the AMMTC on 26 July 2017 wherein ASEAN Member States have agreed to continue to cooperate closely in their efforts to prevent and combat cybercrime, along with terrorism and transnational organized crimes such as trafficking in persons, illicit drug trafficking, money laundering, arms smuggling, and sea piracy;	INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information
57:6	2017- ASEAN-DECLARATION-TO-PREVENT-AND-COMBAT-CYBERCRIME	2017	PURSUANT to the provision of the agreed Work Programme to Implement the ASEAN Plan of Action to Combat Transnational Crimes as adopted during the Preparatory SOMTC for the 10th AMMTC on 28 September 2015 in Kuala Lumpur, Malaysia, particularly on cybercrime components such as information exchange, regulatory and legal matters, law enforcements, capacity building, and extra-regional cooperation;	CAPACITY BUILDING CBM: develop regional approaches to capacity-building STAKEHOLDER COOPERATION for: work with states and/or the private sector/civil society (international and/or domestic) to further cooperate on topics such as law enforcement, prosecution, investment, e-commerce, intellectual property rights, etc.
57:7	2017- ASEAN-DECLARATION-TO-PREVENT-AND-COMBAT-CYBERCRIME	2017	Member State's national framework for cooperation and collaboration in addressing the misuse of cyberspace	CYBER STABILITY for: develop a framework/rules/protocols intended to help prevent the use of ICT tools/practices that are intended to cause harm in order to keep cyberspace secure
57:8	2017- ASEAN-DECLARATION-TO-PREVENT-AND-COMBAT-CYBERCRIME	2017	community education and awareness to prevent cybercrime;	EDUCATION for: implementing [community] education and awareness in order to prevent cybercrime
57:9	2017- ASEAN-DECLARATION-TO-PREVENT-AND-COMBAT-CYBERCRIME	2017	training and research facilities in the educational, professional, technical and administrative spheres;	INFORMATION EXCHANGE CBM: encourage further analysis and study by research institutes and universities on ICT security related matters NORM for: promote cooperation in training to develop ICT/cybersecurity awareness and skills
57:10	2017- ASEAN-DECLARATION-TO-PREVENT-AND-COMBAT-CYBERCRIME	2017	REINFORCE ASEAN's abilities to build and enhance its capabilities to prevent and combat cybercrime by working closely with the INTERPOL Global Complex for Innovation (IGCI), including by voluntarily seconding or stationing cybercrime specialists there; and	CAPACITY BUILDING CBM: enhance capabilities to prevent and combat cybercrime by working with international entities (i.e., INTERPOL)
58:1	2017 - High-Level+Security+Dialogue+With+China+Joint+Statement+4-24-2017	2017	Australia and China agreed to strengthen cooperation on legal and judicial issues and to consult on a regular basis through educational exchanges	INFORMATION EXCHANGE CBM: encouraging exchanges between research and academic institutions

ID	Document	Document Groups	Quotation Content	Codes
58:2	2017 - High-Level+Security+Dialogue+With+China+Joint+Statement+4-24-2017	2017	delegations of officials and judicial officers and through the bilateral Legal Talks and the High-Level Security Dialogue.	INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information
58:3	2017 - High-Level+Security+Dialogue+With+China+Joint+Statement+4-24-2017	2017	commitment to a peaceful, secure, open and cooperative Information and Communications Technology environment.	NORM for: promote an open, secure, stable, accessible, and peaceful cyber space / ICT environment
58:4	2017 - High-Level+Security+Dialogue+With+China+Joint+Statement+4-24-2017	2017	Under the Australia-China High-Level Security Dialogue mechanism, the two countries will establish a mechanism to share information to assist in the fight against and prevention of cybercrime	STAKEHOLDER COOPERATION for: coordinate/cooperate in combatting cybercrime
58:5	2017 - High-Level+Security+Dialogue+With+China+Joint+Statement+4-24-2017	2017	carry out joint law enforcement actions.	STAKEHOLDER COOPERATION for: conduct joint cybersecurity and/or related law enforcement exercises between nation states
58:6	2017 - High-Level+Security+Dialogue+With+China+Joint+Statement+4-24-2017	2017	The two countries will exchange cybersecurity delegations, relevant legal and regulatory documents and learn about each other's legal environment, law enforcement procedures and other relevant circumstances through meetings, communication on individual cases as well as other methods, so as to enhance cooperation and mutual trust.	INFORMATION EXCHANGE for: sharing information regarding national laws/policies/rules/regulations regarding ICTs/cyber space/cybersecurity
58:7	2017 - High-Level+Security+Dialogue+With+China+Joint+Statement+4-24-2017	2017	Australia and China agreed not to conduct or support cyber-enabled theft of intellectual property, trade secrets or confidential business information with the intent of obtaining competitive advantage.	CRITICAL INFRASTRUCTURE against: knowingly support cyberactivity that intentionally damages or impairs the use and operation of critical infrastructure CYBER ATTACK for: preventing ICT-enabled theft of intellectual property (this includes trade secrets and other confidential business information)
59:1	2017 - Australia-India Cyber Policy Dialogue _ DFAT	2017	reaffirmed their commitment to an open, free, secure, stable, peaceful and accessible cyberspace enabling economic growth and innovation	NORM for: promote an open, secure, stable, accessible, and peaceful cyber space / ICT environment NORM for: supporting a free and secure internet / cyber space that supports economic growth and innovation
59:2	2017 - Australia-India Cyber Policy Dialogue _ DFAT	2017	reiterated their support for the multi-stakeholder approach to internet governance	STAKEHOLDER COOPERATION for: coordinate/cooperate in preserving multistakeholder internet governance
59:3	2017 - Australia-India Cyber Policy Dialogue _ DFAT	2017	The two countries agreed that the bilateral Cyber Policy Dialogue provided a strong foundation for existing and future cooperation.	INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information
59:4	2017 - Australia-India Cyber Policy Dialogue _ DFAT	2017	They reaffirmed their commitment to act in accordance with the UNGGE's previous reports and, in particular, the 11 voluntary norms of state behaviour set out in the 2015 report.	UNITED NATIONS for: following the United Nation's (UN) [2015 and or 2013] GGE report's call for all States to be guided in their use of ICTs in relation to the report
59:5	2017 - Australia-India Cyber Policy Dialogue _ DFAT	2017	reaffirmed that responsible behaviour of states in cyberspace is subject to the UN Charter in its entirety and existing international law.	INTERNATIONAL LAW for: applicability of international law to cyberspace
59:6	2017 - Australia-India Cyber Policy Dialogue _ DFAT	2017	further reaffirmed that such behaviour includes respect for human rights and fundamental freedoms	HUMAN RIGHTS for: applicability of international human rights law(s) to cyberspace HUMAN RIGHTS for: respecting human rights and fundamental freedoms; applying them to cyber space / ICT use, etc.
59:7	2017 - Australia-India Cyber Policy Dialogue _ DFAT	2017	Further, the two sides also agreed on a Plan of Action, which identified Points of Contacts on various issues of mutual interest in the area of cyberspace	CONFIDENCE BUILDING CBM: establishing national/international/regional/sub-regional Points of Contact (POCs) is a CBM as well as a prerequisite for the implementation of many other CBMs (i.e., useful for diplomatic, policy, legal and technical exchanges, as well as incident reporting and responses) STATE RESPONSIBILITY CBM: recognize the imperative to have National Action Plans (NAPs) in place in order to contain national policies and strategies intended to prevent and combat cybercrime

ID	Document	Document Groups	Quotation Content	Codes
60:1	2017 - First Australia-Indonesia Cyber Policy Dialogue _ DFAT	2017	reaffirmed their commitment to an open, free and secure internet for economic growth and innovation	NORM for: promote an open, secure, stable, accessible, and peaceful cyber space / ICT environment NORM for: supporting a free and secure internet / cyber space that supports economic growth and innovation
60:2	2017 - First Australia-Indonesia Cyber Policy Dialogue _ DFAT	2017	They welcomed the important contribution of the UN Group of Governmental Experts on norms to date and looked forward to a successful conclusion of the current GGE.	UNITED NATIONS for: following the United Nation's (UN) [2015 and or 2013] GGE report's call for all States to be guided in their use of ICTs in relation to the report
60:3	2017 - First Australia-Indonesia Cyber Policy Dialogue _ DFAT	2017	They agreed to work closely together and with other regional partners on measures to reduce risk in cyberspace. The two countries also agreed that the Cyber Policy Dialogue provided a strong foundation for future cooperation.	INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information
60:4	2017 - First Australia-Indonesia Cyber Policy Dialogue _ DFAT	2017	two sides discussed the full range of cyber issues including the respective visions of the internet and cyberspace, exchanging cyber threat perceptions, policies and strategies, regional and international developments.	INFORMATION EXCHANGE for: sharing information regarding national laws/policies/rules/regulations regarding ICTs/cyber space/cybersecurity
60:5	2017 - First Australia-Indonesia Cyber Policy Dialogue _ DFAT	2017	The dialogue further discussed potential bilateral cooperation to promote a safe, open and secure internet for economic and social development.	INFORMATION EXCHANGE for: furthering future dialogue/cooperation for a safe, open, and secure internet/cyberspace
61:1	2017 - Japan-Australia Cyber Policy Dialogue _ DFAT	2017	Japan and Australia reaffirmed their commitment to work together to harness the opportunity, while managing the risks of our increasingly connected world.	INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information
61:2	2017 - Japan-Australia Cyber Policy Dialogue _ DFAT	2017	We exchanged views on key issues regarding cyber threat trends, national cybersecurity efforts, cooperation in cybersecurity in a regional and multinational context, and cooperation in cybersecurity in a bilateral context.	INFORMATION EXCHANGE for: sharing of good/best practices in relation to ICTs and cybersecurity
61:3	2017 - Japan-Australia Cyber Policy Dialogue _ DFAT	2017	open, free, fair, and secure cyberspace.	NORM for: promote an open, secure, stable, accessible, and peaceful cyber space / ICT environment
61:4	2017 - Japan-Australia Cyber Policy Dialogue _ DFAT	2017	reaffirm that existing international law is applicable in cyberspace	INTERNATIONAL LAW for: applicability of international law to cyberspace
61:5	2017 - Japan-Australia Cyber Policy Dialogue _ DFAT	2017	reaffirm our commitment to promote a strategic framework of international cyber stability consisting of the applicability of existing international law to state behavior in cyberspace	CYBER STABILITY for: develop a framework/rules/protocols intended to help prevent the use of ICT tools/practices that are intended to cause harm in order to keep cyberspace secure
61:6	2017 - Japan-Australia Cyber Policy Dialogue _ DFAT	2017	promotion of agreed voluntary norms of responsible state behavior during peacetime	NORMS CBM: universally agreed upon [voluntary] norms/rules/principles are important for the responsible behavior of States' use of ICTs STATE RESPONSIBILITY for: states should behave responsibly in cyberspace (and use ICTs responsibly) during peacetime
61:7	2017 - Japan-Australia Cyber Policy Dialogue _ DFAT	2017	development and the implementation of practical cyber confidence building measures between states, supported by coordinated capacity building programs.	CAPACITY BUILDING CBM: develop regional approaches to capacity-building CONFIDENCE BUILDING for: develop and implement [practical] cyber confidence building measures (CBMs) between nation states
61:8	2017 - Japan-Australia Cyber Policy Dialogue _ DFAT	2017	Japan and Australia also reaffirmed their commitment to act in accordance with the cumulative reports of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (GGE)	UNITED NATIONS for: following the United Nation's (UN) [2015 and or 2013] GGE report's call for all States to be guided in their use of ICTs in relation to the report
61:9	2017 - Japan-Australia Cyber Policy Dialogue _ DFAT	2017	Going forward, Japan and Australia will continue their cooperation on the further elaboration of international law and norms, confidence building measures and capacity building measures in international and regional fora such as United Nations and ASEAN Regional Forum Inter-Sessional Meeting on Security of and in the Use of Information and Communication Technologies (ARF-ISM on ICTs Security)	STATE RESPONSIBILITY for: dialogue amongst nations by an international body

ID	Document	Document Groups	Quotation Content	Codes
61:10	2017 - Japan-Australia Cyber Policy Dialogue _ DFAT	2017	Moreover, Japan and Australia will continue to enhance cooperation on responding to malicious cyber activities, including deterring and responding to significant cyber incidents, consistent with relevant domestic and international law	CYBER ATTACKS for: responding to requests for help in the event of a cyber attack CYBER ATTACKS for: strengthen tools and resources needed to prepare, deter, defend, and respond to unlawful use of ICTs, cyber attacks / acts of cyber crime and/or terrorism DOMESTIC LAW for: applicability of domestic law to cyber space / ICT usage STATE RESPONSIBILITY & SOVEREIGNTY for: nation states and non-state actors (consistent with their responsibilities and limitations) must respond appropriately to norms violations, ensuring that those who violate norms face predictable and meaningful consequences STATE RESPONSIBILITY for: responding to offensive/illegal/unlawful cyber activities by non state actors if/when discovered
62:1	2017 - JapanUS Cyber Dialogue	2017	ccessible, open, interoperable, reliable and secure cyberspace has contributed to global economic, social and political development.	NORM for: promote an open, secure, stable, accessible, and peaceful cyber space / ICT environment NORM for: supporting a free and secure internet / cyber space that supports economic growth and innovation
62:2	2017 - JapanUS Cyber Dialogue	2017	Japan and the United States recognized that the security and resilience of cyberspace can only be fully achieved through close cooperation and collaboration, both nationally and internationally, with various actors including the private sector, academia, and civil society, and committed to promoting public-private coordination in and between both nations.	INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information STAKEHOLDER COOPERATION for: establishing a standing multistakeholder engagement mechanism in order to address stability issues (this includes adequate involvement and consultation of states, non-state actors such as private sector entities, and civil society)
62:3	2017 - JapanUS Cyber Dialogue	2017	Based on “The Guidelines for Japan-U.S. Defense Cooperation” issued on April 27, 2015, the two countries noted their steady progress on cyberspace cooperation. Japan and the United States also welcomed the progress of the Cyber Defense Policy Working Group (CDPWG) between the Ministry of Defense of Japan and the U.S. Department of Defense.	STATE RESPONSIBILITY for: adhering to rules and regulations agreed upon by previously enacted international law/mandates/treaties
62:4	2017 - JapanUS Cyber Dialogue	2017	consistent with relevant international and domestic law, to continue promoting security, stability and prosperity in cyberspace.	DOMESTIC LAW for: applicability of domestic law to cyber space / ICT usage INTERNATIONAL LAW for: applicability of international law to cyberspace
62:5	2017 - JapanUS Cyber Dialogue	2017	The two countries recognized that critical infrastructure resilience is essential to both countries	CRITICAL INFRASTRUCTURE for: promoting resilience (as related to ICTs,cybersecurity, and related critical infrastructure
62:6	2017 - JapanUS Cyber Dialogue	2017	joint training efforts	STAKEHOLDER COOPERATION for: conduct joint cybersecurity and/or related law enforcement exercises between nation states
62:7	2017 - JapanUS Cyber Dialogue	2017	classifying cyber incident severity	CONFIDENCE BUILDING CBM: classification/categorization of ICT incidents
62:8	2017 - JapanUS Cyber Dialogue	2017	Japan and the United States have closely cooperated in the areas of international law, voluntary, non-binding norms of responsible State behavior in peacetime, and confidence-building measures, including through the 5th United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security and the G7 Ise-Shima Cyber Group (ISCG), and will continue to promote a strategic framework for conflict prevention, cooperation, and stability in cyberspace.	CYBER STABILITY for: develop a framework/rules/protocols intended to help prevent the use of ICT tools/practices that are intended to cause harm in order to keep cyberspace secure NORMS CBM: universally agreed upon [voluntary] norms/rules/principles are important for the responsible behavior of States' use of ICTs STAKEHOLDER COOPERATION for: work with states and/or the private sector/civil society (international and/or domestic) to further cooperate on topics such as law enforcement, prosecution, investment, e-commerce, intellectual property rights, etc. STATE RESPONSIBILITY for: states should behave responsibly in cyberspace (and use ICTs responsibly) during peacetime UNITED NATIONS for: following the United Nation's (UN) [2015 and or 2013] GGE report's call for all States to be guided in their use of ICTs in relation to the report

ID	Document	Document Groups	Quotation Content	Codes
62:9	2017 - JapanUS Cyber Dialogue	2017	deter and respond to malicious cyber activities, consistent with relevant domestic and international law, including the law of State responsibility.	CYBER ATTACKS for: strengthen tools and resources needed to prepare, deter, defend, and respond to unlawful use of ICTs, cyber attacks / acts of cyber crime and/or terrorism CYBER STABILITY for: deterring cyber incidents / attacks
63:1	2017 - Singapore Signs MOU with Australia to Enhance Cybersecurity Collaboration	2017	regular information exchanges on cybersecurity incidents and threats	INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information
63:2	2017 - Singapore Signs MOU with Australia to Enhance Cybersecurity Collaboration	2017	sharing of best practices to promote innovation in cybersecurity,	INFORMATION EXCHANGE for: sharing of good/best practices in relation to ICTs and cybersecurity
63:3	2017 - Singapore Signs MOU with Australia to Enhance Cybersecurity Collaboration	2017	training in cybersecurity skillsets, joint cybersecurity exercises with a focus on the protection of Critical Information Infrastructure	STAKEHOLDER COOPERATION for: conduct joint cybersecurity and/or related law enforcement exercises between nation states
63:4	2017 - Singapore Signs MOU with Australia to Enhance Cybersecurity Collaboration	2017	collaboration on regional cyber capacity building and confidence building measures	CAPACITY BUILDING CBM: develop regional approaches to capacity-building
63:5	2017 - Singapore Signs MOU with Australia to Enhance Cybersecurity Collaboration	2017	Both parties also committed to promote voluntary norms of responsible state behaviour in cyberspace.	NORMS CBM: universally agreed upon [voluntary] norms/rules/principles are important for the responsible behavior of States' use of ICTs
64:1	2017 - ISACA and CSA to Further Develop Singapores Cyber Security Capabilities and Workforce Skills	2017	SACA and the Cyber Security Agency of Singapore (CSA) today signed a Memorandum of Understanding (MOU) to jointly enhance Singapore's cyber security capabilities and workforce, using ISACA-developed training, assessment tools and certi¦cation.	INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information
64:2	2017 - ISACA and CSA to Further Develop Singapores Cyber Security Capabilities and Workforce Skills	2017	both parties will cooperate to bolster professional knowledge and performance in governance, risk and compliance roles and strengthen cyber security content and practice-sharing platforms in Singapore and beyond	INFORMATION EXCHANGE for: establish a formal framework to facilitate professional dialogue
64:3	2017 - ISACA and CSA to Further Develop Singapores Cyber Security Capabilities and Workforce Skills	2017	"There is signi¦cant opportunity in this partnership to develop credentials, content, and resources that address risk management and assessment for ICS and SCADA, as well as rapidly emerging technology such as IoT, arti¦cial intelligence and machine learning.	INFORMATION EXCHANGE for: increasing international cooperation is required to address cyber security risks
65:1	2017 - BRICS+Leaders+Xiamen+Declaration+9-4-17	2017	We note that practical economic cooperation has traditionally served as a foundation of BRICS cooperation, notably through implementing the Strategy for BRICS Economic Partnership and initiatives related to its priority areas such as trade and investment, manufacturing and minerals processing, infrastructure connectivity, financial integration, science, technology and innovation, and Information and Communication Technology (ICT) cooperation	INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information
65:2	2017 - BRICS+Leaders+Xiamen+Declaration+9-4-17	2017	We will enhance joint BRICS research, development and innovation in ICT including the Internet of Things, Cloud computing, Big Data, Data Analytics, Nanotechnology, Artificial Intelligence and 5G and their innovative applications to elevate the level of ICT infrastructure and connectivity in our countries	INFORMATION EXCHANGE CBM: encourage further analysis and study by research institutes and universities on ICT security related matters
65:3	2017 - BRICS+Leaders+Xiamen+Declaration+9-4-17	2017	advocate the establishment of internationally applicable rules for security of ICT infrastructure, data protection and the Internet that can be widely accepted by all parties concerned, and jointly build a network that is safe and secure	NORM for: promote an open, secure, stable, accessible, and peaceful cyber space / ICT environment NORMS CBM: universally agreed upon [voluntary] norms/rules/principles are important for the responsible behavior of States' use of ICTs
65:4	2017 - BRICS+Leaders+Xiamen+Declaration+9-4-17	2017	recognize the need to further increase investment in ICT Research and development	CONFIDENCE BUILDING CBM: further investments in ICT research and development
65:5	2017 - BRICS+Leaders+Xiamen+Declaration+9-4-17	2017	We encourage identification and facilitation of partnership between institutes, organizations, enterprises in the implementation of proof of concepts and pilot projects by leveraging complementary strengths in ICT hardware, software and skills through developing next generation of innovative solutions in the areas of smart cities, health care and energy efficient device, etc. We support active collaboration in implementing the BRICS ICT Development Agenda and Action Plan	STAKEHOLDER COOPERATION CBM: cooperation between states/entities (domestic and/or international) is important for furthering economic relationships/development

ID	Document	Document Groups	Quotation Content	Codes
65:6	2017 - BRICS+Leaders+Xiamen+Declaration+9-4-17	2017	ICT application in agriculture to contribute to stable global agricultural growth and achievement of Sustainable Development Goals.	FOOD SECURITY for: utilizing ICTs in order to ensure food security, food safety, addressing malnutrition, and working towards eliminating hunger and poverty (via agricultural production, productivity, sustainability, management of natural resources, and trade)
65:7	2017 - BRICS+Leaders+Xiamen+Declaration+9-4-17	2017	We appreciate the efforts and contribution of the BRICS Business Council and Business Forum to strengthening our economic cooperation in infrastructure, manufacturing, energy, agriculture, financial services, e-commerce, alignment of technical standards and skills development. We welcome the establishment of a working group on regional aviation within the framework of the Business Council and in this connection acknowledge the Brazil's proposal on an MOU on regional aviation partnership. We encourage business communities and associations to actively participate in BRICS cooperation, and give full play to their role as trade and investment facilitation institutions in promoting mutually beneficial cooperation.	STAKEHOLDER COOPERATION for: work with states and/or the private sector/civil society (international and/or domestic) to further cooperate on topics such as law enforcement, prosecution, investment, e-commerce, intellectual property rights, etc.
65:8	2017 - BRICS+Leaders+Xiamen+Declaration+9-4-17	2017	global governance, counter-terrorism, security in the use of ICTs, energy security, major international and regional hotspots as well as national security and development. We note Brazil's proposal to establish a 3/2/2018 BRICS Leaders Xiamen Declaration https://www.brics2017.org/English/Documents/Summit/201709/t20170908_2021.html 10/26 BRICS Intelligence Forum. We welcome Chair's report to us on the proceedings of the Meeting and encourage the succeeding chairpersonships to continue this exercise. We look forward to enhancing practical security cooperation agreed upon in the above areas.	CAPACITY BUILDING CBM: assign appropriate weight to ICT security awareness and capacity building in development and assistance planning CONFIDENCE BUILDING CBM: recognize importance of ICTs as the key driver of governance, economy, commerce, trade, and social well-being
65:9	2017 - BRICS+Leaders+Xiamen+Declaration+9-4-17	2017	through organized crime by means of money-laundering, supply of weapons, drug trafficking and other criminal activities, dismantling terrorist bases, and countering misuse of the Internet including social media by terrorist entities through misuse of the latest Information and Communication Technologies (ICTs).	CYBER ATTACKS for: strengthen tools and resources needed to prepare, deter, defend, and respond to unlawful use of ICTs, cyber attacks / acts of cyber crime and/or terrorism STAKEHOLDER COOPERATION for: coordinate/cooperate in combatting cybercrime
65:10	2017 - BRICS+Leaders+Xiamen+Declaration+9-4-17	2017	We consider the UN has a central role in developing universally accepted norms of responsible state behavior in the use of ICTs to ensure a peaceful, secure, open, cooperative, stable, orderly, accessible and equitable ICT environment. We emphasize the paramount importance of the principles of international law enshrined in the Charter of the United Nations, particularly the state sovereignty, the political independence, territorial integrity and sovereign equality of states, non-interference in internal affairs of other states and respect for human rights and fundamental freedoms	CYBER STABILITY for: protecting political systems DIGITAL EQUALITY CBM: work towards digital equality and inclusion (i.e., for women and traditionally marginalised groups) - this includes cooperation between the private sector, civil society, and national governments (as well as multilateral banks, and international entities such as the United Nations) HUMAN RIGHTS for: applicability of international human rights law(s) to cyberspace HUMAN RIGHTS for: respecting human rights and fundamental freedoms; applying them to cyber space / ICT use, etc. INTERNATIONAL LAW for: applicability of international law to cyberspace STATE SOVEREIGNTY for: state sovereignty applied to State's ICT activities & ICT infrastructure within their territory UNITED NATIONS CBM: the United Nations (UN) may serve as an international body for decision-making, framework creation/implementation, and when developing and adopting universally agreed upon ICT norms/rules/principles (in order to ensure peace and responsible behavior/ICT use)
65:11	2017 - BRICS+Leaders+Xiamen+Declaration+9-4-17	2017	reaffirm the general approach laid in the eThekwini, Fortaleza, Ufa and Goa declarations in this regard, and recognize the need for a universal regulatory binding instrument on combatting the criminal use of ICTs under the UN auspices as stated in the Ufa Declaration. We note with satisfaction the progress achieved by the Working Group of Experts of the BRICS States on Security in the use of ICTs. We decide to promote cooperation according to the BRICS Roadmap of Practical Cooperation on Ensuring Security in the Use of ICTs or any other mutually agreed mechanism and acknowledge the initiative of the Russian Federation on a BRICS intergovernmental agreement on cooperation in ensuring security in the use of ICTs.	STATE RESPONSIBILITY for: adhering to rules and regulations agreed upon by previously enacted international law/mandates/treaties

ID	Document	Document Groups	Quotation Content	Codes
65:12	2017 - BRICS+Leaders+Xiamen+Declaration+9-4-17	2017	encourage greater application of ICTs to improve the level of health service provision	STATE RESPONSIBILITY CBM: encourage greater application of ICTs to improve the level of health service provision
66:1	2017 - Joint Communiqué - 2nd Canada-China High-Level National Security and Rule of Law Dialogue _ Prime Minister of Canada	2017	The two sides agreed, on the basis of the Joint Communiqué of the 1 Canada-China High- Level National Security and Rule of Law Dialogue, to take further measures aimed at strengthening bilateral cooperation in the areas of law enforcement, judicial and security cooperation	INFORMATION EXCHANGE for: sharing information regarding national laws/policies/rules/regulations regarding ICTs/cyber space/cybersecurity STAKEHOLDER COOPERATION for: work with states and/or the private sector/civil society (international and/or domestic) to further cooperate on topics such as law enforcement, prosecution, investment, e-commerce, intellectual property rights, etc.
66:2	2017 - Joint Communiqué - 2nd Canada-China High-Level National Security and Rule of Law Dialogue _ Prime Minister of Canada	2017	The two sides agreed to strengthen cooperation, on the basis of the Treaty between Canada and the People's Republic of China on Mutual Legal Assistance in Criminal Matters. The two sides also had candid discussions on an extradition treaty in the context of the rule of law	STATE RESPONSIBILITY for: adhering to rules and regulations agreed upon by previously enacted international law/mandates/treaties
66:3	2017 - Joint Communiqué - 2nd Canada-China High-Level National Security and Rule of Law Dialogue _ Prime Minister of Canada	2017	he two sides agreed to strengthen cooperation on counter-terrorism, including through a deepening of existing bilateral counter-terrorism consultations, and working to combat the use of the internet to incite, recruit, Ýnance or plan and implement terrorist activities.	CYBER ATTACKS for: strengthen tools and resources needed to prepare, deter, defend, and respond to unlawful use of ICTs, cyber attacks / acts of cyber crime and/or terrorism STAKEHOLDER COOPERATION for: coordinate/cooperate in combatting cybercrime STAKEHOLDER COOPERATION for: work / intensify cooperation against criminal/terrorist use of ICTs
66:4	2017 - Joint Communiqué - 2nd Canada-China High-Level National Security and Rule of Law Dialogue _ Prime Minister of Canada	2017	The two sides agreed that neither country's government would conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other conÝdential business information, with the intent of providing competitive advantages to companies or commercial sectors.	CYBER ATTACK for: preventing ICT-enabled theft of intellectual property (this includes trade secrets and other confidential business information)
66:5	2017 - Joint Communiqué - 2nd Canada-China High-Level National Security and Rule of Law Dialogue _ Prime Minister of Canada	2017	The two sides also agreed that the next round of High-Level National Security and Rule of Law Dialogue should take place in Beijing in 2018.	INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information
67:1	2017 - China, Germany hold security dialogue to strengthen cooperation - People's Daily Online	2017	China and Germanyheld their first high-level security dialogue in Beijing Tuesday, with both countries agreeing to deepen security communication and cooperation.	INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information
67:2	2017 - China, Germany hold security dialogue to strengthen cooperation - People's Daily Online	2017	against terrorism and transnational organized crime,	STAKEHOLDER COOPERATION for: coordinate/cooperate in combatting cybercrime STAKEHOLDER COOPERATION for: work / intensify cooperation against criminal/terrorist use of ICTs
68:1	2017 - Second high-level UK-China security dialogue_ February 2017 - GOV.UK	2017	The dialogue covered a wide range of security issues including cyber; counter-terrorism; and organised crime. The two delegations also held a detailed exchange of views on pressing global security challenges, including the situation in Syria and the importance of implementing UN Security Council Resolutions on the Democratic People's Republic of Korea (DPRK)	INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information
68:2	2017 - Second high-level UK-China security dialogue_ February 2017 - GOV.UK	2017	regular coordination on cyber security-related issues in order to prevent cyber commercial espionage and related transnational criminal activity	INFORMATION EXCHANGE for: increasing international cooperation is required to address cyber security risks STAKEHOLDER COOPERATION for: coordinate/cooperate in combatting cybercrime
69:1	2017 - ChinaRussia Cyber Dialogue	2017	Xi Jinping pointed out that both China and Russia are good neighbors connecting by mountains and rivers, good friends offering mutual support and assistance, and good partners collaborating sincerely. Bilateral comprehensive strategic partnership of coordination is in the fundamental interests of the two countries and peoples	INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information

ID	Document	Document Groups	Quotation Content	Codes
69:3	2017 - ChinaRussia Cyber Dialogue	2017	The two heads of state agreed to make joint efforts to deepen bilateral comprehensive strategic partnership of coordination, and build high-level and strong China-Russia relations into a booster of development and revitalization between both countries as well as a ballast stone for world peace and stability. The two sides vowed to abide by the "China-Russia Treaty on Good-neighborliness, Friendship and Cooperation" no matter how the international situation changes, follow consensus reached by the two heads of state, support each other's efforts in safeguarding core interests in sovereignty, security and territorial integrity, support each country to step onto a development road conforming to own national conditions, and back up each other's development and revitalization. Both sides agreed to bring into play the strategic guiding role of the two heads of state in bilateral relations, maintain close high-level exchanges, well use bilateral cooperation mechanism, enhance coordination between legislative institutions, and strengthen friendly exchanges and cooperation between the two governmental departments, local level and non-governmental organizations.	STAKEHOLDER COOPERATION CBM: form bilateral and multilateral cooperation initiatives to build on established partnerships/relationships
69:4	2017 - ChinaRussia Cyber Dialogue	2017	Both sides agreed to carry out close and effective coordination in international and regional affairs, strengthen communication and coordination under frameworks including the UN and the UN Security Council, the Shanghai Cooperation Organization, BRICS, the G20, Asia-Pacific Economic Cooperation and Asia-Europe Meeting	STAKEHOLDER COOPERATION for: support other international and/or regional cooperative partnerships STATE RESPONSIBILITY for: dialogue amongst nations by an international body
70:1	2017 - 4th European Union - United States Cyber Dialogue	2017	Following the exchange, the EU and U.S. idenΘfed synergies and commiΣed to conΘnue to share informaΘon and to coordinate on an on-going basis to ensure the uΘlizaΘon of these synergies for the beneft of the U.S., the EU, EU Member States, and the mulΘ- stakeholder community.	INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information
70:2	2017 - 4th European Union - United States Cyber Dialogue	2017	stable and secure cyberspace	NORM for: promote an open, secure, stable, accessible, and peaceful cyber space / ICT environment
70:3	2017 - 4th European Union - United States Cyber Dialogue	2017	reafrmed the applicaΘon of exisΘng internaΘonal law to State behaviour in cyberspace	INTERNATIONAL LAW for: applicability of international law to cyberspace
70:4	2017 - 4th European Union - United States Cyber Dialogue	2017	adherence to voluntary, non-binding norms of responsible State behaviour in cyberspace during peaceΘme	NORMS CBM: universally agreed upon [voluntary] norms/rules/principles are important for the responsible behavior of States' use of ICTs STATE RESPONSIBILITY for: states should behave responsibly in cyberspace (and use ICTs responsibly) during peacetime
70:5	2017 - 4th European Union - United States Cyber Dialogue	2017	endorsed the work that has been done by the UN Group of Governmental Experts on Developments in the Field of InformaΘon and TelecommunicaΘons in the Context of InternaΘonal Security (UNGGE), including its landmark 2013 and 2015 reports	UNITED NATIONS for: following the United Nation's (UN) [2015 and or 2013] GGE report's call for all States to be guided in their use of ICTs in relation to the report
70:6	2017 - 4th European Union - United States Cyber Dialogue	2017	The EU and U.S. marked the importance of adherence to the framework of responsible State behaviour idenΘfed in the UNGGE reports	NORMS CBM: national declarations of adherence to the normative framework of responsible State behavior could build trust and confidence between states
70:7	2017 - 4th European Union - United States Cyber Dialogue	2017	discussed ways to hold accountable States that act contrary to that framework.	STATE RESPONSIBILITY AND SOVEREIGNTY CBM: hold other nation states / entities accountable for actions that may be contrary to the international consensus on responsible State behavior in cyberspace
70:8	2017 - 4th European Union - United States Cyber Dialogue	2017	as well as the important work on the development and implementaΘon of cyber confdence building measures to reduce mispercepΘon and the risk of escalaΘon when using informaΘon and communicaΘons technologies (ICTs	STATE RESPONSIBILITY CBM: transnational consulting to reduce risk of misperception, escalation, and conflict
70:9	2017 - 4th European Union - United States Cyber Dialogue	2017	discussed the need to strengthen the measures to prevent, detect and respond to malicious acΘviΘes in cyberspace,	CYBER ATTACKS for: strengthen tools and resources needed to prepare, deter, defend, and respond to unlawful use of ICTs, cyber attacks / acts of cyber crime and/or terrorism CYBER STABILITY for: deterring cyber incidents / attacks
70:10	2017 - 4th European Union - United States Cyber Dialogue	2017	infuence the behaviour of actors in cyberspace to refrain from malicious acΘviΘes.	CYBER ATTACKS against: [non-state actors] engaging in offensive/harmful cyber operations of any kind
70:11	2017 - 4th European Union - United States Cyber Dialogue	2017	digital divide to enable economic growth, social developments	DIGITAL EQUALITY for: closing the digital divide (i.e., by empowering communities to benefit from digital opportunities)
70:12	2017 - 4th European Union - United States Cyber Dialogue	2017	d increasing cyber resilience towards cyber threats.	CRITICAL INFRASTRUCTURE for: promoting resilience (as related to ICTs,cybersecurity, and related critical infrastructure

ID	Document	Document Groups	Quotation Content	Codes
70:13	2017 - 4th European Union - United States Cyber Dialogue	2017	investments, along with partners to increase the global capaciӨes to prevent and miӨgate cyber threats and to invesӨgate and prosecute cyber criminals	CONFIDENCE BUILDING CBM: further investments in ICT research and development STAKEHOLDER COOPERATION for: work with states and/or the private sector/civil society (international and/or domestic) to further cooperate on topics such as law enforcement, prosecution, investment, e-commerce, intellectual property rights, etc.
70:14	2017 - 4th European Union - United States Cyber Dialogue	2017	EU and U.S. expressed the need to strengthen internaӨonal cooperaӨon, coordinaӨon, and sharing of best pracӨces to maximize the economic and social beneft enabled by the Internet and the use of ICTs, including within the Global Forum for Cyber ExperӨse	INFORMATION EXCHANGE for: sharing information regarding national laws/policies/rules/regulations regarding ICTs/cyber space/cybersecurity INFORMATION EXCHANGE for: sharing of good/best practices in relation to ICTs and cybersecurity STAKEHOLDER COOPERATION CBM: cooperation between states/entities (domestic and/or international) is important for furthering economic relationships/development STATE RESPONSIBILITY for: dialogue amongst nations by an international body
70:15	2017 - 4th European Union - United States Cyber Dialogue	2017	The EU and U.S. reafrmed the importance of the Budapest ConvenӨon as a solid basis for naӨonal legislaӨon and internaӨonal cooperaӨon in fghӨng cybercrime.	CONFIDENCE BUILDING CBM: adopt legislative basis for combatting cybercrime (i.e., the Budapest Convention)
70:16	2017 - 4th European Union - United States Cyber Dialogue	2017	mulӨ- stakeholder approach to Internet governance that includes the parӨcipaӨon and contribuӨons of all stakeholders.	STAKEHOLDER COOPERATION for: coordinate/cooperate in preserving multistakeholder internet governance STAKEHOLDER COOPERATION for: encourage participation of other stakeholders such as the private sector, academia, and civil society orgs (as appropriate) for CBM and/or norm creation and implementation
70:17	2017 - 4th European Union - United States Cyber Dialogue	2017	Both sides stressed that no single enӨty, company, government, or inter-governmental organizaӨon should seek to control the Internet.	CYBERSPACE STABILITY against: any single entity/company/government/inter-governmental organization should seek control of the internet
70:18	2017 - 4th European Union - United States Cyber Dialogue	2017	transparent, inclusive and accessible to all stakeholders and welcomed the eforts to capture and package the content of the Internet Governance Forum, such as the European Commission work on the Global Internet Policy Observatory (GIPO), and the Friends of the Internet Governance Forum.	CONFIDENCE BUILDING CBM: voluntary transparency STAKEHOLDER COOPERATION for: support other international and/or regional cooperative partnerships
70:19	2017 - 4th European Union - United States Cyber Dialogue	2017	same rights and freedoms people have ofine must also be protected online.	INDIVIDUAL RIGHTS for: acknowledging that the same rights that individuals have offline are also protected online
70:20	2017 - 4th European Union - United States Cyber Dialogue	2017	promote the applicaӨon of exisӨng internaӨonal human rights law and the ongoing work in the UN and the Freedom Online CoaliӨon. The EU and U.S. reafrmed their strong commitment to an open Internet on which individuals can exercise their human rights and fundamental freedoms, including the freedoms of expression and associaӨon, and to condemn any efort to exploit the Internet for malicious intent including repression.	HUMAN RIGHTS for: applicability of international human rights law(s) to cyberspace HUMAN RIGHTS for: respecting human rights and fundamental freedoms; applying them to cyber space / ICT use, etc.
71:1	2017 - Communique+G20+Finance+Ministers+and+Central+Bank+Governors	2017	promote the resilience of financial services and institutions in G20 jurisdictions against the malicious use of ICT, including from countries outside the G20.	DIGITAL ECONOMY for: promote resilience of financial services and institutions against malicious use of ICTs
71:2	2017 - Communique+G20+Finance+Ministers+and+Central+Bank+Governors	2017	We support the work of the Global Partnership for Financial Inclusion (GPFI) to advance financial inclusion, especially of vulnerable groups, and Small and Medium-sized Enterprises' (SMEs) participation in sustainable global value chains. We encourage an adequate coverage of opportunities and challenges of digital financial inclusion in the updated G20 Financial Inclusion Action Plan. We encourage G20 and non-G20 countries to take steps to implement the G20 High-Level Principles for Digital Financial Inclusion	DIGITAL ECONOMY for: take steps to ensure digital financial inclusion in regards to technologically enabled finances (i.e., e-commerce) DIGITAL EQUALITY for: closing the digital divide (i.e., by empowering communities to benefit from digital opportunities)
71:3	2017 - Communique+G20+Finance+Ministers+and+Central+Bank+Governors	2017	increased access to financial products in a digital world	ACCESS CBM: access to the internet is an important enabler of development./growth/innovation

ID	Document	Document Groups	Quotation Content	Codes
72:1	2017 - G20-leaders-declaration___blob=publicationFile&v=11	2017	bridge digital divides along multiple dimensions, including income, age, geography and gender	DIGITAL EQUALITY for: closing the digital divide (i.e., by empowering communities to benefit from digital opportunities) DIGITAL EQUALITY for: closing the gender digital divide (focusing on women and girls, but also those a part of gender subgroups such as the LGBTQI+ communiy)
72:2	2017 - G20-leaders-declaration___blob=publicationFile&v=11	2017	We will strive to ensure that all our citizens are digitally connected by 2025 and especially welcome infrastructure development in low-income countries in that regard	ACCESS for: every adult should have affordable access to digital networks (including digitally-enabled financial and health services) ASSIST for: adopting appropriate policies and measures so that developing countries benefit from the advantages of technological progress (and do not suffer from lack of early adoption) ASSISTANCE CBM: provide assistance and training to developing countries to improve cybsecurity and ICT use
72:3	2017 - G20-leaders-declaration___blob=publicationFile&v=11	2017	Digital transformation is a driving force of global, innovative, inclusive and sustainable growth and can contribute to reducing inequality and achieving the goals of the 2030 Agenda for Sustainable Development	ACCESS CBM: access to the internet is an important enabler of development./growth/innovation
72:4	2017 - G20-leaders-declaration___blob=publicationFile&v=11	2017	We will promote digital literacy and digital skills in all forms of education and life-long learning	EDUCATION for: implementing [community] education and awareness in order to prevent cybercrime EDUCATION for: include cybersecurity courses in school curricula (i.e., primary school, degree courses in undergrad, professional education, and trainings EDUCATION for: increased eduation, [digital] literacy, and awareness regarding digital rights and ways to exercise/protect them
72:5	2017 - G20-leaders-declaration___blob=publicationFile&v=11	2017	will promote better access to financial resources and services and a more entrepreneurial friendly environment.	DIGITAL ECONOMY for: take steps to ensure digital financial inclusion in regards to technologically enabled finances (i.e., e-commerce)
72:6	2017 - G20-leaders-declaration___blob=publicationFile&v=11	2017	aim to foster favourable conditions for the development of the digital economy and recognise the need to ensure effective competition to foster investment and innovation.	DIGITAL ECONOMY for: fostering safe and secure competition in the digital economy
72:7	2017 - G20-leaders-declaration___blob=publicationFile&v=11	2017	products and services that are based on the principles of openness, transparency and consensus and standards should not act as barriers to trade, competition or innovation.	PRODUCT CBM: transparency and dialogue regarding ICT vulnerabilities and identified harmful hidden functions in ICT products
72:8	2017 - G20-leaders-declaration___blob=publicationFile&v=11	2017	Trust in digital technologies requires effective consumer protection, intellectual property rights, transparency, and security in the use of ICT	CYBER ATTACK for: preventing ICT-enabled theft of intellectual property (this includes trade secrets and other confidential business information) PRODUCT for: developers and producers of products and services should prioritize security and stability
72:9	2017 - G20-leaders-declaration___blob=publicationFile&v=11	2017	We support the free flow of information while respecting applicable legal frameworks for privacy, data protection and intellectual property rights.	ACCESS for: support the free flow of information while respecting applicable legal frameworks for privacy and data protection
72:10	2017 - G20-leaders-declaration___blob=publicationFile&v=11	2017	We are committed to help ensure a secure ICT environment in which all sectors are able to enjoy its benefits and reaffirm the importance of collectively addressing issues of security in the use of ICT	CONFIDENCE BUILDING CBM: address issues [related to cyber space/cybersecurity/ICTs] CYBER STABILITY for: maintaining a secure, safe, and trustable ICT environment NORM for: promote an open, secure, stable, accessible, and peaceful cyber space / ICT environment
72:11	2017 - G20-leaders-declaration___blob=publicationFile&v=11	2017	We will constructively engage in WTO discussions relating to E-commerce and in other international fora with responsibilities related to various aspects of digital trade to foster digital economy development and trade	STATE RESPONSIBILITY for: dialogue amongst nations by an international body
72:12	2017 - G20-leaders-declaration___blob=publicationFile&v=11	2017	Intensified and concerted action is needed to enhance the ability of developing and least developed countries to more fully engage in digital trade	ASSISTANCE CBM: provide assistance and training to developing countries to improve cybsecurity and ICT use
72:14	2017 - G20-leaders-declaration___blob=publicationFile&v=11	2017	An open and resilient financial system, grounded in agreed international standards,	DIGITAL ECONOMY for: promote resilience of financial services and institutions against malicious use of ICTs

ID	Document	Document Groups	Quotation Content	Codes
72:15	2017 - G20-leaders-declaration___blob=publicationFile&v=11	2017	Digitalisation and access to ICT serve as powerful catalysts for the economic empowerment and inclusion of women and girls. Access to STEM (Science, Technology, Engineering and Mathematics) related trainings and occupations is therefore key to establish an enabling environment for women's empowerment. We welcome the launch of the #eSkills4Girls initiative to promote opportunities and equal participation for women and girls in the digital economy, in particular in low income and developing countries (see Annex)	DIGITAL EQUALITY for: gender diversity should be taken into account when technologes are designed
72:16	2017 - G20-leaders-declaration___blob=publicationFile&v=11	2017	In order to achieve food security, we are committed to increase agricultural productivity and resilience in a sustainable manner, while aiming to protect, manage and use efficiently water and water-related ecosystems. In order to harness the potential of ICT, we stress the need for strengthened cooperation on ICT in agriculture and underline the importance of access to high-speed digital services for farmers and of adequately serving rural areas	FOOD SECURITY for: utilizing ICTs in order to ensure food security, food safety, addressing malnutrition, and working towards eliminating hunger and poverty (via agricultural production, productivity, sustainability, management of natural resources, and trade)
73:1	2017 - g7-taormina-leaders-communique	2017	We endorsed the Joint Communiqué, the Declaration on Responsible States Behavior in Cyberspace, and the StatementonNon-ProliferationandDisarmamentoftheForeignMinisters'meetinginLucca,andfurtherdiscussed issuesandcrisesthatareмostseriouslythreateningthesecurityandwell-beingofourcitizensandglobalstability	STATE RESPONSIBILITY for: adhering to rules and regulations agreed upon by previously enacted international law/mandates/treaties
73:2	2017 - g7-taormina-leaders-communique	2017	protectanaccessible,open,interoperable,reliableandsecurecyberspace	CONFIDENCE BUILDING CBM: promote the use of ICTs for peaceful purposes NORM for: promote an open, secure, stable, accessible, and peaceful cyber space / ICT environment
73:3	2017 - g7-taormina-leaders-communique	2017	anditsvast benefitsforeconomicgrowthandprosperity	ACCESS CBM: access to the internet is an important enabler of development./growth/innovation
73:4	2017 - g7-taormina-leaders-communique	2017	Wewillworktogetherandwithotherpartnerstotacklecyberattacks andmitigatetheirimpactonourcriticalinfrastructuresandthewell-beingofoursocieties.	CRITICAL INFRASTRUCTURE for: promoting resilience (as related to ICTs,cybersecurity, and related critical infrastructure CRITICAL INFRASTRUCTURE for: protecting critical infrastructures INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information STAKEHOLDER COOPERATION for: support other international and/or regional cooperative partnerships
73:5	2017 - g7-taormina-leaders-communique	2017	TheNextProductionRevolution(NPR)offers anextraordinaryopportunitytoincreasecompetitiveness andto boostaninnovation-drivengrowth.Byreshapingourexistingproductionsystems,theNPRcanindeedallowallfirms – includingmicro,smallandmedium-sizedenterprises(MSMEs) – andhelppeopleacrossallsectorsandregionsto reapthebenefitsofinnovationanddigitalizationandenhancewomen'sopportunitiestopursueSTEMcareers	DIGITAL EQUALITY for: closing the gender digital divide (focusing on women and girls, but also those a part of gender subgroups such as the LGBTQI+ communiy)
74:1	2017 - g7 declaration on cyberspace	2017	We remain committed to an accessible, open, interoperable, reliable and secure cyberspace	NORM for: promote an open, secure, stable, accessible, and peaceful cyber space / ICT environment
74:2	2017 - g7 declaration on cyberspace	2017	We recognize the enormous benefits for economic growth and prosperity that we and all others derive from cyberspace as an extraordinary tool for economic, social and political development	ACCESS CBM: access to the internet is an important enabler of development./growth/innovation NORM for: supporting a free and secure internet / cyber space that supports economic growth and innovation
74:3	2017 - g7 declaration on cyberspace	2017	We encourage all States to engage in law-abiding, norm-respecting and confidence-building behaviour in their use of ICT	CONFIDENCE BUILDING for: develop and implement [practical] cyber confidence building measures (CBMs) between nation states
74:4	2017 - g7 declaration on cyberspace	2017	Cooperative approaches would also contribute to the fight against the use of cyberspace by non-State actors for terrorist and other criminal purposes.	CYBER ATTACKS for: strengthen tools and resources needed to prepare, deter, defend, and respond to unlawful use of ICTs, cyber attacks / acts of cyber crime and/or terrorism STAKEHOLDER COOPERATION for: coordinate/cooperate in combatting cybercrime STAKEHOLDER COOPERATION for: work / intensify cooperation against criminal/terrorist use of ICTs
74:5	2017 - g7 declaration on cyberspace	2017	For these reasons, the G7 set an ambitious course in promoting security and stability in cyberspace and the protection of human rights, through "The Principles and Actions on Cyber" endorsed in Ise-Shima on 26 and 27 May 2016.	STATE RESPONSIBILITY for: adhering to rules and regulations agreed upon by previously enacted international law/mandates/treaties

ID	Document	Document Groups	Quotation Content	Codes
74:6	2017 - g7 declaration on cyberspace	2017	We continue to call upon all States to be guided in their use of Information and Communications Technologies (ICTs) by the cumulative reports of the United Nations Groups of Governmental Experts in the Field of Information and Telecommunications in the Context of International Security (UN-GGE).	UNITED NATIONS for: following the United Nation's (UN) [2015 and or 2013] GGE report's call for all States to be guided in their use of ICTs in relation to the report
74:7	2017 - g7 declaration on cyberspace	2017	We recognize the urgent necessity of increased international cooperation to promote security and stability in cyberspace, including on measures aimed at reducing the malicious use of ICTs by State and non-State actors	CYBER ATTACKS against: [non-state actors] engaging in offensive/harmful cyber operations of any kind INFORMATION EXCHANGE AND TRANSPARENCY for: cooperate/exchange guidelines and/or best practices against disruptions by non-State actors INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information
74:8	2017 - g7 declaration on cyberspace	2017	strategic framework for conflict prevention, cooperation and stability in cyberspace	CYBER STABILITY for: develop a framework/rules/protocols intended to help prevent the use of ICT tools/practices that are intended to cause harm in order to keep cyberspace secure INFORMATION EXCHANGE for: establish a formal framework to facilitate professional dialogue
74:9	2017 - g7 declaration on cyberspace	2017	consisting of the recognition of the applicability of existing international law to State behavior in cyberspace,	INTERNATIONAL LAW for: applicability of international law to cyberspace
74:11	2017 - g7 declaration on cyberspace	2017	development and the implementation of practical cyber confidence building measures (CBMs) between States;	CONFIDENCE BUILDING for: develop and implement [practical] cyber confidence building measures (CBMs) between nation states
74:12	2017 - g7 declaration on cyberspace	2017	We also reaffirm that the same rights that people have offline must also be protected online	INDIVIDUAL RIGHTS for: acknowledging that the same rights that individuals have offline are also protected online
74:13	2017 - g7 declaration on cyberspace	2017	reaffirm the applicability of international human rights law in cyberspace	HUMAN RIGHTS for: applicability of international human rights law(s) to cyberspace
74:14	2017 - g7 declaration on cyberspace	2017	international law also provides a framework for States' responses to wrongful acts that do not amount to an armed attack - these may include malicious cyber activities. Among other lawful responses, a State that is the victim of an internationally wrongful act may, in certain circumstances, resort to proportionate countermeasures, including measures conducted via ICTs, against the State responsible for the wrongful act in order to cause the responsible State to comply with its international obligations;	STATE RESPONSIBILITY AND SOVEREIGNTY CBM: hold other nation states / entities accountable for actions that may be contrary to the international consensus on responsible State behavior in cyberspace
74:15	2017 - g7 declaration on cyberspace	2017	In this respect, States cannot escape legal responsibility for internationally wrongful cyber acts by perpetrating them through proxies.	CYBER ATTACKS against: using proxies for [international] wrongful cyber acts CYBER ATTACKS disagreement: invoking countermeasures in response to cyber attacks
74:16	2017 - g7 declaration on cyberspace	2017	We also recognized that 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;	INTERNATIONAL LAW disagreement: the right of self-defense
74:17	2017 - g7 declaration on cyberspace	2017	publicly explain their views on how existing international law applies to States' activities in cyberspace to the greatest extent possible in order to improve transparency and give rise to more settled expectations of State behavior;	INTERNATIONAL LAW CBM: states should publicly express their views on how existing international law applies to activities in cyberspace (in order to improve transparency, etc.) INTERNATIONAL LAW disagreement: how to implement/enfoce a treaty regarding norms/rules/principles (considering that there is uncertainty about how international law applies to cyberspace)
74:18	2017 - g7 declaration on cyberspace	2017	confidence building measures on States' use of ICTs are also an essential element to strengthen international peace and security.	CONFIDENCE BUILDING for: CBMs' value in increasing transparency, predictability, and stability
74:19	2017 - g7 declaration on cyberspace	2017	n addition, we support the promotion of voluntary, non-binding norms of responsible State behavior in cyberspace during peacetime, which can reduce risks to international peace, security and stability.	NORMS CBM: universally agreed upon [voluntary] norms/rules/principles are important for the responsible behavior of States' use of ICTs STATE RESPONSIBILITY for: states should behave responsibly in cyberspace (and use ICTs responsibly) during peacetime
74:20	2017 - g7 declaration on cyberspace	2017	Such norms do not seek to limit or prohibit any action that is otherwise consistent with international law	INTERNATIONAL LAW NORMS against: norms should not seek to limit or prohibit any action that is otherwise consistent with international law

ID	Document	Document Groups	Quotation Content	Codes
74:21	2017 - g7 declaration on cyberspace	2017	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;	CYBER STABILITY for: develop a framework/rules/protocols intended to help prevent the use of ICT tools/practices that are intended to cause harm in order to keep cyberspace secure UNITED NATIONS CBM: the United Nations (UN) may serve as an international body for decision-making, framework creation/implementation, and when developing and adopting universally agreed upon ICT norms/rules/principles (in order to ensure peace and responsible behavior/ICT use)
74:22	2017 - g7 declaration on cyberspace	2017	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;	STATE RESPONSIBILITY for: considering all relevant information in the event of an ICT incident
74:23	2017 - g7 declaration on cyberspace	2017	States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs;	CYBER ATTACKS against: states knowingly allowing their territory to be used for internationally wrongful acts using ICTs
74:24	2017 - g7 declaration on cyberspace	2017	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;	STAKEHOLDER COOPERATION for: work with states and/or the private sector/civil society (international and/or domestic) to further cooperate on topics such as law enforcement, prosecution, investment, e-commerce, intellectual property rights, etc.
74:25	2017 - g7 declaration on cyberspace	2017	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;	HUMAN RIGHTS for: respecting human rights and fundamental freedoms; applying them to cyber space / ICT use, etc.
74:26	2017 - g7 declaration on cyberspace	2017	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	CRITICAL INFRASTRUCTURE against: knowingly damaging critical infrastructure
74:27	2017 - g7 declaration on cyberspace	2017	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;	CRITICAL INFRASTRUCTURE for: protecting critical infrastructures
74:28	2017 - g7 declaration on cyberspace	2017	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;	CYBER ATTACKS for: responding to requests for help in the event of a cyber attack
74:29	2017 - g7 declaration on cyberspace	2017	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;	DIGITAL ECONOMY for: further ensuring the integrity of the ICT supply chain
74:30	2017 - g7 declaration on cyberspace	2017	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;	PRODUCT CBM: transparency and dialogue regarding ICT vulnerabilities and identified harmful hidden functions in ICT products PRODUCT for: creating transparent procedures and frameworks to asses whether and when to disclose not publicly known vulnerabilities or flaws in their information systems and/or technologies
74:31	2017 - g7 declaration on cyberspace	2017	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.	CYBER ATTACKS against: states using authorized emergency response teams to engage in malicuous / harmful international activity CYBER ATTACKS against: targeting emergency response teams
74:32	2017 - g7 declaration on cyberspace	2017	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.	STATE RESPONSIBILITY & SOVEREIGNTY against: conducting or supporting ICT-enabled theft of intellectual property, trade secrets, or other confidential business info
75:1	2017 - OSCE ministerial council	2017	Noting the immense opportunities that information and communication technologies provide for social and economic development, and that they continue to grow in importance for the international community	ACCESS CBM: access to the internet is an important enabler of development./growth/innovation

ID	Document	Document Groups	Quotation Content	Codes
75:2	2017 - OSCE ministerial council	2017	Reaffirming that efforts by OSCE participating States to reduce the risks of conflict stemming from the use of information and communication technologies will be consistent with: international law, including, inter alia, the UN Charter and the International Covenant on Civil and Political Rights; the Helsinki Final Act; and their responsibilities to respect human rights and fundamental freedoms,	HUMAN RIGHTS for: applicability of international human rights law(s) to cyberspace HUMAN RIGHTS for: respecting human rights and fundamental freedoms; applying them to cyber space / ICT use, etc. INTERNATIONAL LAW for: applicability of international law to cyberspace STATE RESPONSIBILITY for: adhering to rules and regulations agreed upon by previously enacted international law/mandates/treaties
75:3	2017 - OSCE ministerial council	2017	Reiterating in the context of security of and in the use of information and communication technologies the central role of the United Nations, and taking note of the continued relevance of the 2010, 2013 and 2015 reports of the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security,	UNITED NATIONS CBM: the United Nations (UN) may serve as an international body for decision-making, framework creation/implementation, and when developing and adopting universally agreed upon ICT norms/rules/principles (in order to ensure peace and responsible behavior/ICT use) UNITED NATIONS for: following the United Nation's (UN) [2015 and or 2013] GGE report's call for all States to be guided in their use of ICTs in relation to the report
75:4	2017 - OSCE ministerial council	2017	Continue to implement all decisions on confidence-building measures adopted by the OSCE to reduce the risks of conflict stemming from the use of information and communication technologies to contribute to an open, secure, stable, accessible and peaceful information and communication technologies environment in line with OSCE commitments;	CONFIDENCE BUILDING for: develop and implement [practical] cyber confidence building measures (CBMs) between nation states NORM for: promote an open, secure, stable, accessible, and peaceful cyber space / ICT environment STAKEHOLDER COOPERATION CBM: it is important for other stakeholders such as regional and sub-regional bodies/entities be used to create, promote, and implement CBMs
75:5	2017 - OSCE ministerial council	2017	Identify ways of strengthening and optimizing the work of the OSCE as a practical platform for reducing risks of conflict stemming from the use of information and communication technologies, and at the same time continuing the work of the cross-dimensional Informal Working Group established pursuant to Permanent Council Decision No. 1039;	CYBER STABILITY for: continuing to work towards reducing the risk of conflict stemming from ICT use
75:6	2017 - OSCE ministerial council	2017	Encourage executive OSCE structures, within their mandates and available resources, to assist participating States, upon their request, in the implementation of the OSCE confidence-building measures to reduce the risk of conflict stemming from the use of information and communication technologies, and to enhance pertinent national capabilities and processes;	ASSISTANCE for: assist partner states (and/or others), upon request, with the implementation of CBMs
75:7	2017 - OSCE ministerial council	2017	Invite the OSCE Partners for Co-operation to enhance dialogue on efforts to reduce the risks of conflict stemming from the use of information and communication technologies.	INFORMATION EXCHANGE for: establish a formal framework to facilitate professional dialogue INFORMATION EXCHANGE for: furthering future dialogue/cooperation for a safe, open, and secure internet/cyberspace INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information STATE RESPONSIBILITY for: dialogue amongst nations by an international body
76:1	2017 - Singapore+Signs+Memorandum+Of+Cooperation+On+Cybersecurity+With+Japan+at+the+Sidelines+of+SICW+2017+9-18-2017	2017	regular policy dialogues, information exchanges,	INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information
76:2	2017 - Singapore+Signs+Memorandum+Of+Cooperation+On+Cybersecurity+With+Japan+at+the+Sidelines+of+SICW+2017+9-18-2017	2017	collaborations to enhance cybersecurity awareness	NORM for: promote cooperation in training to develop ICT/cybersecurity awareness and skills

ID	Document	Document Groups	Quotation Content	Codes
76:3	2017 - Singapore+Signs+Memorandum+Of+Cooperation+On+Cybersecurity+With+Japan+at+the+Sidelines+of+SICW+2017+9-18-2017	2017	joint regional capacity building efforts	CAPACITY BUILDING CBM: develop regional approaches to capacity-building
76:4	2017 - Singapore+Signs+Memorandum+Of+Cooperation+On+Cybersecurity+With+Japan+at+the+Sidelines+of+SICW+2017+9-18-2017	2017	as well as sharing of best practices between both countries	INFORMATION EXCHANGE for: sharing of good/best practices in relation to ICTs and cybersecurity
77:1	2017 - Singapore+Signs+Joint+Declaration+of+Intent+on+Cybersecurity+Cooperation+With+Germany+7-6-2017	2017	regular information exchanges	INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information
77:2	2017 - Singapore+Signs+Joint+Declaration+of+Intent+on+Cybersecurity+Cooperation+With+Germany+7-6-2017	2017	joint training and research;	NORM for: promote cooperation in training to develop ICT/cybersecurity awareness and skills
77:3	2017 - Singapore+Signs+Joint+Declaration+of+Intent+on+Cybersecurity+Cooperation+With+Germany+7-6-2017	2017	sharing of best practices to promote innovation in cybersecurity.	INFORMATION EXCHANGE for: sharing of good/best practices in relation to ICTs and cybersecurity
77:4	2017 - Singapore+Signs+Joint+Declaration+of+Intent+on+Cybersecurity+Cooperation+With+Germany+7-6-2017	2017	Both parties also commit to promote voluntary norms of responsible state behaviour in cyberspace.	NORMS CBM: universally agreed upon [voluntary] norms/rules/principles are important for the responsible behavior of States' use of ICTs
78:1	2017 - Joint+Statement+from+President+Donald+J.+Trump+and+Prime+Minister+Justin+Trudeau+2-13-2017	2017	We therefore commit to further cooperation to enhance critical infrastructure security, cyber incident management, public awareness, private sector engagement, and capacity building initiatives.	CAPACITY BUILDING CBM: develop regional approaches to capacity-building CRITICAL INFRASTRUCTURE for: promoting resilience (as related to ICTs,cybersecurity, and related critical infrastructure CRITICAL INFRASTRUCTURE for: protecting critical infrastructures INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information NORM for: promote cooperation in training to develop ICT/cybersecurity awareness and skills STAKEHOLDER COOPERATION for: encourage participation of other stakeholders such as the private sector, academia, and civil society orgs (as appropriate) for CBM and/or norm creation and implementation
79:1	2017 - First U.S.-China Law Enforcement and Cybersecurity Dialogue _ OPA _ Department of Justice	2017	Both sides will continue their implementation of the consensus reached by the Chinese and American Presidents in 2015 on U.S.-China cybersecurity cooperation	STATE RESPONSIBILITY for: adhering to rules and regulations agreed upon by previously enacted international law/mandates/treaties
79:2	2017 - First U.S.-China Law Enforcement and Cybersecurity Dialogue _ OPA _ Department of Justice	2017	that timely responses should be provided to requests for information and assistance concerning malicious cyber activities;	CYBER ATTACKS for: responding to requests for help in the event of a cyber attack STATE RESPONSIBILITY for: timely responses to requests for information

ID	Document	Document Groups	Quotation Content	Codes
79:3	2017 - First U.S.-China Law Enforcement and Cybersecurity Dialogue _ OPA _ Department of Justice	2017	hat neither country's government will conduct or knowingly support cyber-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	CYBER ATTACK for: preventing ICT-enabled theft of intellectual property (this includes trade secrets and other confidential business information) STATE RESPONSIBILITY & SOVEREIGNTY against: conducting or supporting ICT-enabled theft of intellectual property, trade secrets, or other confidential business info
79:4	2017 - First U.S.-China Law Enforcement and Cybersecurity Dialogue _ OPA _ Department of Justice	2017	to make common effort to further identify and promote appropriate norms of state behavior in cyberspace within the international community	NORMS CBM: national declarations of adherence to the normative framework of responsible State behavior could build trust and confidence between states
79:5	2017 - First U.S.-China Law Enforcement and Cybersecurity Dialogue _ OPA _ Department of Justice	2017	to maintain a high-level joint dialogue mechanism on fighting cybercrime and related issues	INFORMATION EXCHANGE for: establish a formal framework to facilitate professional dialogue INFORMATION EXCHANGE for: furthering future dialogue/cooperation for a safe, open, and secure internet/cyberspace STAKEHOLDER COOPERATION for: coordinate/cooperate in combatting cybercrime
79:6	2017 - First U.S.-China Law Enforcement and Cybersecurity Dialogue _ OPA _ Department of Justice	2017	enhance law enforcement communication on cyber security incidents and to mutually provide timely responses.	STAKEHOLDER COOPERATION for: work with states and/or the private sector/civil society (international and/or domestic) to further cooperate on topics such as law enforcement, prosecution, investment, e-commerce, intellectual property rights, etc.
79:7	2017 - First U.S.-China Law Enforcement and Cybersecurity Dialogue _ OPA _ Department of Justice	2017	as well as considering future efforts on cybersecurity of critical infrastructure.	CRITICAL INFRASTRUCTURE for: promoting resilience (as related to ICTs,cybersecurity, and related critical infrastructure CRITICAL INFRASTRUCTURE for: protecting critical infrastructures
80:1	2017 - Key+Outcomes+of+the+U.S.-Japan-ROK+Trilateral+Vice+Foreign+Ministerial+Meetings+1-5-2017	2017	Our cyber policy experts consulted trilaterally on December 19, 2016 in Washington, DC regarding the cybersecurity of critical infrastructure, including a discussion of cyber trends and threats to critical infrastructure as well as a scenario-based discussion on responding to malicious cyber activities.	CRITICAL INFRASTRUCTURE for: promoting resilience (as related to ICTs,cybersecurity, and related critical infrastructure CRITICAL INFRASTRUCTURE for: protecting critical infrastructures INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information STATE RESPONSIBILITY for: adhering to rules and regulations agreed upon by previously enacted international law/mandates/treaties
81:1	2017 - Joint+UK-Australia+Statement+on+Cyber+Cooperation+7-11-2017	2017	We recognise that the pace and development of new technologies and applications, in conjunction with greater access, is delivering significant opportunities for both economic and social development.	NORM for: supporting a free and secure internet / cyber space that supports economic growth and innovation
81:2	2017 - Joint+UK-Australia+Statement+on+Cyber+Cooperation+7-11-2017	2017	nternational stability framework for cyberspace based on the application of existing international law, agreed voluntary norms of responsible state behaviour and confidence building measures, supported by co-ordinated capacity building programmes.	CONFIDENCE BUILDING for: promote cooperation in regional confidence-building measures (CBMs) INTERNATIONAL LAW for: applicability of international law to cyberspace NORMS CBM: universally agreed upon [voluntary] norms/rules/principles are important for the responsible behavior of States' use of ICTs
81:3	2017 - Joint+UK-Australia+Statement+on+Cyber+Cooperation+7-11-2017	2017	deter, mitigate and attribute malicious cyber attacks by criminals, state actors and their proxies, including those that seek to interfere in the internal democratic processes of states	CYBER ATTACKS for: strengthen tools and resources needed to prepare, deter, defend, and respond to unlawful use of ICTs, cyber attacks / acts of cyber crime and/or terrorism CYBER STABILITY for: deterring cyber incidents / attacks CYBER STABILITY for: protecting political systems
81:4	2017 - Joint+UK-Australia+Statement+on+Cyber+Cooperation+7-11-2017	2017	We reaffirm our commitment to a free, open, peaceful and secure cyberspace	NORM for: promote an open, secure, stable, accessible, and peaceful cyber space / ICT environment
81:5	2017 - Joint+UK-Australia+Statement+on+Cyber+Cooperation+7-11-2017	2017	human rights and fundamental freedoms, and the application of international humanitarian law to cyber operations in armed conflict	HUMAN RIGHTS for: applicability of international human rights law(s) to cyberspace HUMAN RIGHTS for: respecting human rights and fundamental freedoms; applying them to cyber space / ICT use, etc.
81:6	2017 - Joint+UK-Australia+Statement+on+Cyber+Cooperation+7-11-2017	2017	right of states to act in self-defence in response to an armed attack	CYBER ATTACKS disagreement: invoking countermeasures in response to cyber attacks INTERNATIONAL LAW disagreement: the right of self-defense

ID	Document	Document Groups	Quotation Content	Codes
81:7	2017 - Joint+UK-Australia+Statement+on+Cyber+Cooperation+7-11-2017	2017	he law of state responsibility applies to cyber operations in peacetime, including the availability of the doctrine of countermeasures in response to internationally wrongful acts	STATE RESPONSIBILITY for: states should behave responsibly in cyberspace (and use ICTs responsibly) during peacetime
81:8	2017 - Joint+UK-Australia+Statement+on+Cyber+Cooperation+7-11-2017	2017	We recognise that an increasing number of states are developing operational cyber capabilities. We assert states' legitimate right to develop these capabilities, and emphasise their obligation to ensure their use is governed in accordance with international law	CAPACITY BUILDING for: states have a legitimate right to develop operational cyber capabilities DIGITAL GOVERNANCE for: states are obligated to ensure that the use of ICTs/cyber capabilities is governed
81:9	2017 - Joint+UK-Australia+Statement+on+Cyber+Cooperation+7-11-2017	2017	We will promote operationalisation of norms of responsible state behaviour recommended in the 2015 report of the UN Group of Governmental Experts on developments in the field of information and telecommunications in the context of international security. We will focus on positive practical measures that states can take to put these voluntary norms into practice. We will also implement confidence building measures that can build trust between responsible states. In doing so we recognise that transparency is the first step to establishing mutual trust and provides a foundation for measures available to all states, whatever their stage of development. We are committed to working through the OSCE and ASEAN Regional Forum as a way of contributing to peace and understanding in cyberspace.	STAKEHOLDER COOPERATION for: support other international and/or regional cooperative partnerships UNITED NATIONS for: following the United Nation's (UN) [2015 and or 2013] GGE report's call for all States to be guided in their use of ICTs in relation to the report
81:10	2017 - Joint+UK-Australia+Statement+on+Cyber+Cooperation+7-11-2017	2017	building resilience to cyber threats,	CRITICAL INFRASTRUCTURE for: promoting resilience (as related to ICTs,cybersecurity, and related critical infrastructure
81:11	2017 - Joint+UK-Australia+Statement+on+Cyber+Cooperation+7-11-2017	2017	strengthening law enforcement responses in line with the Budapest Convention on Cybercrime	CONFIDENCE BUILDING CBM: adopt legislative basis for combatting cybercrime (i.e., the Budapest Convention)
82:1	2017 - Statement of Extraordinary Summit of the Cooperation Council for the Arab States of the Gulf (GCC) and the United States of America _ The White House	2017	cyber security, and protecting infrastructure	CRITICAL INFRASTRUCTURE for: protecting critical infrastructures INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information
83:1	2017 - India-Germany+Joint+Statement+During+the+visit+of+Prime+Minister+to+Germany+5-30-2017	2017	They welcomed the regular holding of annual German-Indian Cyber consultations since 2015, geared towards cooperation to strengthen the bilateral cyber relationship as laid out in the Joint Declaration of Intent on German-Indian Cooperation on Cyber Policy.	INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information STAKEHOLDER COOPERATION CBM: form bilateral and multilateral cooperation initiatives to build on established partnerships/relationships
83:2	2017 - India-Germany+Joint+Statement+During+the+visit+of+Prime+Minister+to+Germany+5-30-2017	2017	Both leaders reiterated their commitment to promote shared values such as respect for human rights and fundamental freedoms, democratic governance, equality, the rule of law, and multilateral cooperation.	DIGITAL EQUALITY adopted: working towards digital equality and inclusion HUMAN RIGHTS for: respecting human rights and fundamental freedoms; applying them to cyber space / ICT use, etc.
84:1	2017 - Joint+Statement+From+the+Ministry+of+Economy++Trade+and+Industry+of+Japan+and+the+Ministry+of+Economy+and+Industry+of+the+State+of+Israel+5-3-2017	2017	Japanese experts and decision makers will participate in training programs in Israel.	INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information STAKEHOLDER COOPERATION CBM: exchange of personnel
84:2	2017 - Joint+Statement+From+the+Ministry+of+Economy++Trade+and+Industry+of+Japan+and+the+Ministry+of+Economy+and+Industry+of+the+State+of+Israel+5-3-2017	2017	Joint training between both countries will be held by Israel National Cyber Directorate (INCD) for the purpose of enhancing cybersecurity skills and sharing experiences of both countries	NORM for: promote cooperation in training to develop ICT/cybersecurity awareness and skills

ID	Document	Document Groups	Quotation Content	Codes
84:3	2017 - Joint+Statement+From+the+Ministry+of+Economy++Trade+and+Industry+of+Japan+and+the+Ministry+of+Economy+and+Industry+of+the+State+of+Israel+5-3-2017	2017	Both sides will promote a workshop of experts from government entities and industry aimed at sharing information and views on the current situation in cybersecurity and responses to cyberattacks in order to enhance cooperation for sharing best practices on protection and mitigation against cyberattacks.	INFORMATION EXCHANGE CBM: encouraging exchanges between research and academic institutions
85:1	2017 - EU+Council+Conclusions+on+the+Joint+Communication+Resilience,+Deterrence+and+Defence+Building+strong+cybersecurity+for+the+EU	2017	RECOGNISING the importance of cybersecurity for the prosperity, growth and security of the EU and integrity of our free and democratic societies and their underpinning processes in the digital age, both by protecting rule of law and human rights and fundamental freedoms of every individual	ACCESS CBM: access to the internet is an important enabler of development./growth/innovation HUMAN RIGHTS for: respecting human rights and fundamental freedoms; applying them to cyber space / ICT use, etc.
85:2	2017 - EU+Council+Conclusions+on+the+Joint+Communication+Resilience,+Deterrence+and+Defence+Building+strong+cybersecurity+for+the+EU	2017	UNDERLINING the need to address cybersecurity with a coherent approach at national, EU and global level, as cyber threats can have an impact on our democracy, prosperity, stability and security	CONFIDENCE BUILDING CBM: address issues [related to cyber space/cybersecurity/ICTs]
85:3	2017 - EU+Council+Conclusions+on+the+Joint+Communication+Resilience,+Deterrence+and+Defence+Building+strong+cybersecurity+for+the+EU	2017	continuously promote an open, global, free, peaceful and secure cyberspace,	NORM for: promote an open, secure, stable, accessible, and peaceful cyber space / ICT environment
85:4	2017 - EU+Council+Conclusions+on+the+Joint+Communication+Resilience,+Deterrence+and+Defence+Building+strong+cybersecurity+for+the+EU	2017	access to information, data protection, privacy and security,	ACCESS CBM: access to the internet is an important enabler of development./growth/innovation ACCESS for: support the free flow of information while respecting applicable legal frameworks for privacy and data protection
85:5	2017 - EU+Council+Conclusions+on+the+Joint+Communication+Resilience,+Deterrence+and+Defence+Building+strong+cybersecurity+for+the+EU	2017	RECOGNISING that international law, including the UN Charter in its entirety, international humanitarian law and human rights law apply in cyberspace and thereby UNDERLINING the need to continue the efforts to ensure that international law is upheld in cyberspace;	HUMAN RIGHTS for: applicability of international human rights law(s) to cyberspace INTERNATIONAL LAW for: applicability of international law to cyberspace
85:6	2017 - EU+Council+Conclusions+on+the+Joint+Communication+Resilience,+Deterrence+and+Defence+Building+strong+cybersecurity+for+the+EU	2017	RECALLING its Conclusions on the EU Cyber security Strategy2, on Internet governance3 Strengthening EU Cyber Resilience4, on Cyber Diplomacy5 and on a Framework for Joint EU Diplomatic Response to Malicious Cyber Activities6, on improving criminal justice in cyberspace7; on Security and Defence in the context of the EU Global Strategy8, the Joint Framework on countering hybrid threats9, and on the mid-term review of the renewed European Union Internal Security Strategy 2015-202010;	STATE RESPONSIBILITY for: adhering to rules and regulations agreed upon by previously enacted international law/mandates/treaties
85:7	2017 - EU+Council+Conclusions+on+the+Joint+Communication+Resilience,+Deterrence+and+Defence+Building+strong+cybersecurity+for+the+EU	2017	RECOGNISING that the framework provided by the Council of Europe Convention on Cybercrime (the Budapest Convention), provides a solid basis among a diverse group of countries to use an effective legal standard for the different national legislation and for international cooperation addressing cybercrime;	CONFIDENCE BUILDING CBM: adopt legislative basis for combatting cybercrime (i.e., the Budapest Convention)
85:8	2017 - EU+Council+Conclusions+on+the+Joint+Communication+Resilience,+Deterrence+and+Defence+Building+strong+cybersecurity+for+the+EU	2017	INVITES the Member States, the EU institutions, agencies and bodies to work together, respecting each other's' areas of competence and the principle of subsidiarity and proportionality,	INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information

ID	Document	Document Groups	Quotation Content	Codes
85:9	2017 - EU+Council+Conclusions+on+the+Joint+Communication+Resilience,+Deterrence+and+Defence+Building+strong+cybersecurity+for+the+EU	2017	sufficient financing respecting the available resources to support building cyber resilience and cybersecurity research and development efforts across the EU, as well as to strengthen cooperation to prevent, deter, detect and respond to cyber threats and to be able to respond jointly to large-scale cyber incidents and malicious cyber activities across the EU	CAPACITY BUILDING CBM: pioritize ICT security awareness and capacity-building in national plans and budgets
85:10	2017 - EU+Council+Conclusions+on+the+Joint+Communication+Resilience,+Deterrence+and+Defence+Building+strong+cybersecurity+for+the+EU	2017	strong and trusted encryption is highly important for properly ensuring human rights and fundamental freedoms in EU and for public trust in the Digital Single Market,	PRODUCT for: governments and private sector should cooperate in identifying vulnerabilities within encryption/encrypted products (and then notify developers/vendors of these issues)
85:11	2017 - EU+Council+Conclusions+on+the+Joint+Communication+Resilience,+Deterrence+and+Defence+Building+strong+cybersecurity+for+the+EU	2017	conduct regular strategic cybersecurity exercises in different Council formations, building upon the experience gained during the EU CYBRID 2017 and	NORM for: promote cooperation in training to develop ICT/cybersecurity awareness and skills
85:12	2017 - EU+Council+Conclusions+on+the+Joint+Communication+Resilience,+Deterrence+and+Defence+Building+strong+cybersecurity+for+the+EU	2017	protecting critical infrastructures	CRITICAL INFRASTRUCTURE for: protecting critical infrastructures
85:13	2017 - EU+Council+Conclusions+on+the+Joint+Communication+Resilience,+Deterrence+and+Defence+Building+strong+cybersecurity+for+the+EU	2017	STRESSES that legislative work to strengthen cybersecurity certification on the EU level will have to meet the needs of the market and the users	CONFIDENCE BUILDING CBM: legislative work to strengthen cybsersecurity certification will have to meet the needs of the market and its users
85:14	2017 - EU+Council+Conclusions+on+the+Joint+Communication+Resilience,+Deterrence+and+Defence+Building+strong+cybersecurity+for+the+EU	2017	enhancing cybersecurity certification in the EU, the whole spectrum of security requirements should be covered, up to the highest ones, where resistance against attackers' capabilities has to be demonstrated. Key success factors would be ensuring a reliable, transparent and independent process for security certification to promote the availability of trusted and secure devices, software and services within the Single Market and beyond; recognising European industry, governments and evaluation specialists' respective expertise through European and global standards 14; respecting Member States' role in the certification process in particular as regards to evaluation at higher security levels and especially in relation to essential security needs and skills assessment. Such certification framework should also ensure that any EU-wide certification scheme is proportionate to the level of assurance needed for the use of ICT products, services and/or systems involved, and it enables cross-border trading for businesses of all scales to develop and sell new products, both within the EU and outside the EU markets.	EDUCATION - CERTIFICATION for: enhancing cybersecurity certification as a whole spectrum (cover a wide variety of security requirements, up to the highest ones)
85:16	2017 - EU+Council+Conclusions+on+the+Joint+Communication+Resilience,+Deterrence+and+Defence+Building+strong+cybersecurity+for+the+EU	2017	WELCOMES the emphasis put within the Joint Communication on education, cyber hygiene and awareness in Member States and EU;	STATE RESPONSIBILITY for: nation-state enacted laws and/or regulations to ensure basic cyber protocols/cleanliness/hygiene
85:17	2017 - EU+Council+Conclusions+on+the+Joint+Communication+Resilience,+Deterrence+and+Defence+Building+strong+cybersecurity+for+the+EU	2017	everyone's responsibility in cybersecurity and INVITES the EU and its Member States to promote digital skills and media literacy helping users to protect their digital information online and raise their awareness on the risks when placing personal data on the Internet;	EDUCATION for: increased eduation, [digital] literacy, and awareness regarding digital rights and ways to exercise/protect them

ID	Document	Document Groups	Quotation Content	Codes
85:18	2017 - EU+Council+Conclusions+on+the+Joint+Communication+Resilience,+Deterrence+and+Defence+Building+strong+cybersecurity+for+the+EU	2017	rioritise cyber-awareness in information campaigns and stimulate cybersecurity as part of academic, education and vocational training programmes. Particular focus should be put on youth education and digital skills fostering, to create future-proof professionals ready for the challenges in security, economy and services;	EDUCATION for: implementing [community] education and awareness in order to prevent cybercrime EDUCATION for: include cybersecurity courses in school curricula (i.e., primary school, degree courses in undergrad, professional education, and trainings
85:19	2017 - EU+Council+Conclusions+on+the+Joint+Communication+Resilience,+Deterrence+and+Defence+Building+strong+cybersecurity+for+the+EU	2017	to create an effective cooperation network of education points of contact (POCs) under the umbrella of ENISA. The PoCs network should aim to enhance coordination and exchange of best practices among Member States on cybersecurity education and awareness, as well as training, exercise and capacity building;	CONFIDENCE BUILDING CBM: establishing national/international/regional/sub-regional Points of Contact (POCs) is a CBM as well as a prerequisite for the implementation of many other CBMs (i.e., useful for diplomatic, policy, legal and technical exchanges, as well as incident reporting and responses)
85:20	2017 - EU+Council+Conclusions+on+the+Joint+Communication+Resilience,+Deterrence+and+Defence+Building+strong+cybersecurity+for+the+EU	2017	to advance efforts in opening specialised high-level cybersecurity programmes in order to fill the current gap in cybersecurity professionals in EU	CAPACITY BUILDING CBM: advance efforts in opening specialized high-level cybersecurity programs in order to fill the current gap in cybersecurity professionals
85:21	2017 - EU+Council+Conclusions+on+the+Joint+Communication+Resilience,+Deterrence+and+Defence+Building+strong+cybersecurity+for+the+EU	2017	efficient EU-level response to large-scale cyber incidents and crises, while respecting the competences of Member States, and the need for cybersecurity to be mainstreamed into existing crisis management mechanisms at the EU level17.	EMERGENCY RESPONSE for: mainstreaming cybersecurity emergency management into existing crisis management mechanisms
85:22	2017 - EU+Council+Conclusions+on+the+Joint+Communication+Resilience,+Deterrence+and+Defence+Building+strong+cybersecurity+for+the+EU	2017	Cybersecurity Emergency Response Fund alongside the existing efforts of Member States and respecting the available resources (especially within the EU Multiannual Financial Framework) to help Member States to respond to and mitigate large scale cyber incidents, provided that the Member State had put in place a prudent system of cybersecurity prior to the incident, including full implementation of the NIS Directive and mature risk management and supervisory frameworks at the national level;	EMERGENCY RESPONSE for: establish a Cybersecurity Emergency Response fund (pooling together resources from one nation or multiple within a partnership)
85:23	2017 - EU+Council+Conclusions+on+the+Joint+Communication+Resilience,+Deterrence+and+Defence+Building+strong+cybersecurity+for+the+EU	2017	to be responsive to the threat of 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;	CYBER ATTACK for: preventing ICT-enabled theft of intellectual property (this includes trade secrets and other confidential business information)
85:24	2017 - EU+Council+Conclusions+on+the+Joint+Communication+Resilience,+Deterrence+and+Defence+Building+strong+cybersecurity+for+the+EU	2017	address crimes in cyberspace, including those in the Darkweb, child sexual exploitation online as well as fraud and counterfeiting of non-cash means of payment, notably by aiming at creating an improved intelligence picture, conducting joint investigations and sharing operational support;	STAKEHOLDER COOPERATION for: conduct joint cybersecurity and/or related law enforcement exercises between nation states STAKEHOLDER COOPERATION for: coordinate/cooperate in combatting cybercrime STAKEHOLDER COOPERATION for: work with states and/or the private sector/civil society (international and/or domestic) to further cooperate on topics such as law enforcement, prosecution, investment, e-commerce, intellectual property rights, etc.
85:26	2017 - EU+Council+Conclusions+on+the+Joint+Communication+Resilience,+Deterrence+and+Defence+Building+strong+cybersecurity+for+the+EU	2017	UNDERLINES the importance of providing the law enforcement with tools that enable to detect, investigate and prosecute cybercrime, so that crimes committed in the cyberspace would not go unnoticed or unpunished and WELCOMES the contribution of the European Judicial Cybercrime Network in the fight against crime through judicial authorities cooperation;	CYBER ATTACKS for: strengthen tools and resources needed to prepare, deter, defend, and respond to unlawful use of ICTs, cyber attacks / acts of cyber crime and/or terrorism

ID	Document	Document Groups	Quotation Content	Codes
85:27	2017 - EU+Council+Conclusions+on+the+Joint+Communication+Resilience,+Deterrence+and+Defence+Building+strong+cybersecurity+for+the+EU	2017	global internet governance decisions within the multi-stakeholder community, such as ensuring swiftly accessible and accurate WHOIS databases of IP-addresses and domain names, so that law enforcement capabilities and public interests are safeguarded;	DIGITAL GOVERNANCE for: digital governance must adapt and respond to the needs of citizens DIGITAL GOVERNANCE for: digital governance structures need to focus on enhancing confidence and trust in digital technologies, ensuring security and creating stability and predictability in cyberspace STAKEHOLDER COOPERATION for: coordinate/cooperate in preserving multistakeholder internet governance
85:29	2017 - EU+Council+Conclusions+on+the+Joint+Communication+Resilience,+Deterrence+and+Defence+Building+strong+cybersecurity+for+the+EU	2017	52. RECOGNISES the role of the United Nations in further developing norms for responsible state behaviour in cyberspace and recalls that the outcomes of the United Nations Group of Governmental Experts discussions over the years have articulated a consensual set of norms and recommendations20, which the General Assembly has repeatedly endorsed, and which States should take as a basis for responsible state behaviour in cyberspace;	UNITED NATIONS for: following the United Nation's (UN) [2015 and or 2013] GGE report's call for all States to be guided in their use of ICTs in relation to the report
85:30	2017 - EU+Council+Conclusions+on+the+Joint+Communication+Resilience,+Deterrence+and+Defence+Building+strong+cybersecurity+for+the+EU	2017	RECOGNISES that those norms of responsible State behaviour include that States should not knowingly allow their territory to be used for internationally wrongful acts, should respond to appropriate requests for assistance by another State whose critical infrastructure is subject to malicious ICT acts emanating from their territory and that States should take appropriate measures to protect their critical infrastructure from ICT threats	CRITICAL INFRASTRUCTURE for: protecting critical infrastructures CYBER ATTACKS against: states knowingly allowing their territory to be used for internationally wrongful acts using ICTs CYBER ATTACKS for: responding to requests for help in the event of a cyber attack STATE RESPONSIBILITY & SOVEREIGNTY for: ensuring that one's territory is not used by non-State actors to commit internationally wrongful acts using ICTs
86:1	2017 - Joint Communiqué of the 15th Meeting of the Foreign Ministers of the Russian Federation, the Republic of India and the People's Republic of China	2017	prevent misuse of Information and Communication Technologies (ICTs) for terrorist purposes. We underline the primary and leading role and responsibility of States in preventing and countering terrorism and extremism and reiterate that all States should take adequate measures to prevent terrorist activities from their territory.	STAKEHOLDER COOPERATION for: work / intensify cooperation against criminal/terrorist use of ICTs
86:2	2017 - Joint Communiqué of the 15th Meeting of the Foreign Ministers of the Russian Federation, the Republic of India and the People's Republic of China	2017	We consider the UN has a role in developing universally accepted norms of responsible state behaviour in the use of Information and Communication Technologies (ICTs) to ensure a peaceful, secure, open, cooperative, stable, orderly, accessible and equitable ICT environment. In the use of ICTs, we emphasize the paramount importance of the principles of international law enshrined in the Charter of the United Nations, particularly the state sovereignty, the political independence, territorial integrity and sovereign equality of states, non-interference in internal afairs of other states and respect for human rights and fundamental freedoms. We recognize the need for a universal regulatory binding instrument on combating the criminal use of ICTs. We believe that all states should participate on an equal footing in the evolution and functioning of the Internet and its governance, bearing in mind the need to involve relevant stakeholders in their respective roles and responsibilities. The structures that manage and regulate the critical Internet resources need to be made more representative and inclusive. We will continue to work together to contribute to the secure, open, peaceful and cooperative use of ICTs on the basis of equal participation of the international community in its management.	UNITED NATIONS CBM: the United Nations (UN) may serve as an international body for decision-making, framework creation/implementation, and when developing and adopting universally agreed upon ICT norms/rules/principles (in order to ensure peace and responsible behavior/ICT use)
87:1	2017 - Russian+South+Africa+on+Maintaining+International+Information+Security+9-4-2017	2017	including the use of information-communications technologies for perpetrating acts of aggression, violating the sovereignty, security and territorial integrity of states, for interfering in their domestic affairs, damaging their economies and also for terrorist and other criminal purposes.	STAKEHOLDER COOPERATION for: coordinate/cooperate in combatting cybercrime STAKEHOLDER COOPERATION for: work / intensify cooperation against criminal/terrorist use of ICTs
87:2	2017 - Russian+South+Africa+on+Maintaining+International+Information+Security+9-4-2017	2017	advancing the relevant norms of international law, implementing joint research and development projects and training experts in this feld.	INFORMATION EXCHANGE CBM: encourage further analysis and study by research institutes and universities on ICT security related matters INFORMATION EXCHANGE CBM: encouraging exchanges between research and academic institutions INTERNATIONAL LAW for: applicability of international law to cyberspace NORM for: promote cooperation in training to develop ICT/cybersecurity awareness and skills

ID	Document	Document Groups	Quotation Content	Codes
87:3	2017 - Russian+South+Africa+on+Maintaining+International+Information+Security+9-4-2017	2017	This implies the creation of a joint system for responding to threats in this sphere,	CYBER ATTACKS for: strengthen tools and resources needed to prepare, deter, defend, and respond to unlawful use of ICTs, cyber attacks / acts of cyber crime and/or terrorism
88:1	2016 - 11th IGF Chairs Summary_Final	2016	increasing meaningful, empowering access to the Internet	ACCESS CBM: access to the internet is an important enabler of development./growth/innovation
88:2	2016 - 11th IGF Chairs Summary_Final	2016	digital literacy and the development of local and culturally diverse and relevant content is fundamental for inclusive growth. An emerging consensus has developed amongst the IGF community that the Internet's core values of openness, freedom, resilience, safety, and decentralisation are fundamental for enabling inclusive and sustainable growth	EDUCATION for: increased eduation, [digital] literacy, and awareness regarding digital rights and ways to exercise/protect them NORM for: promote an open, secure, stable, accessible, and peaceful cyber space / ICT environment
88:3	2016 - 11th IGF Chairs Summary_Final	2016	international cooperation and strategic partnerships	INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information
88:4	2016 - 11th IGF Chairs Summary_Final	2016	bridge digital divides and provide crucial new opportunities for people living in poverty, women and girls, children, persons with disabilities, older persons, indigenous peoples, marginalised groups, as well as rural communities that still lack acceptable and quality access and training in the use of ICTs and the Internet.	DIGITAL EQUALITY CBM: work towards digital equality and inclusion (i.e., for women and traditionally marginalised groups) - this includes cooperation between the private sector, civil society, and national governments (as well as multilateral banks, and international entities such as the United Nations) DIGITAL EQUALITY for: closing the digital divide (i.e., by empowering communities to benefit from digital opportunities) DIGITAL EQUALITY for: closing the gender digital divide (focusing on women and girls, but also those a part of gender subgroups such as the LGBTQI+ communiy) NORM for: promote cooperation in training to develop ICT/cybersecurity awareness and skills
88:5	2016 - 11th IGF Chairs Summary_Final	2016	human rights and their connections with Internet policy and governance; while discussions about the importance of human rights on the Internet have similarly become increasingly prominent at the IGF. This year, increased attention has also been paid to the importance of civil and political rights - including the ways in which the promotion and protection of these rights can support sustainable development.	HUMAN RIGHTS for: respecting human rights and fundamental freedoms; applying them to cyber space / ICT use, etc.
88:6	2016 - 11th IGF Chairs Summary_Final	2016	transition of the IANA functions5 to the multistakeholder community in October of 2016, only a few months prior to the 11th IGF, marks an important milestone for the multistakeholder Internet governance community	STAKEHOLDER COOPERATION for: coordinate/cooperate in preserving multistakeholder internet governance
88:7	2016 - 11th IGF Chairs Summary_Final	2016	t. Stakeholders stressed the need for cybersecurity measures to be implemented in cooperation with all stakeholders and international expert bodies; with the IGF providing a unique space for such collaborative efforts. Security professionals, law enforcement agencies, programmers, and business people, among others, have to work together in order to address new threats and challenges to online security for both individuals and organizations. Cyberattacks, cybercrime and issues related to privacy and surveillance are challenges that require urgent collaboration and cooperation as well.	STAKEHOLDER COOPERATION CBM: it is important for other stakeholders such as regional and sub-regional bodies/entities be used to create, promote, and implement CBMs STAKEHOLDER COOPERATION for: encourage participation of other stakeholders such as the private sector, academia, and civil society orgs (as appropriate) for CBM and/or norm creation and implementation
88:8	2016 - 11th IGF Chairs Summary_Final	2016	Internet of Things and artificial intelligence have the potential to bring about ground- breaking benefits to mankind and our quality of life. The challenge is to foster this continuous development and to enable the IoT to further grow into the Internet and Internet governance processes. Issues and challenges such as standardisation, interoperability, and security are very similar to issues the Internet dealt with in its young history, and offer substantial opportunities for multistakeholder cooperation and mutual learning	ARTIFICIAL INTELLIGENCE CBM: incorporate cooperation through a multistakeholder lense in designing and applying standards and principles (such as transparency and responsibility) towards artificial intelligent systems and related technologies ARTIFICIAL INTELLIGENCE for: identify and address risks associated with artificial intelligence and related technologies
88:9	2016 - 11th IGF Chairs Summary_Final	2016	Organizers of these 32 open forums10 – a session type traditionally reserved for governments, IGOs and relevant international organizations – included the Governments of China, Cuba, Egypt, Germany, Indonesia, Japan and Mexico, as well as the African Union, European Commission, Organization of American States (OAS), OECD, ITU and UNESCO, among many others. A delegation of 12 members of the European Parliament, the largest ever to come to an IGF, was also in attendance.	INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information

ID	Document	Document Groups	Quotation Content	Codes
88:10	2016 - 11th IGF Chairs Summary_Final	2016	Topics like privacy and big data; the Internet of Things; dealing with radicalised expression; the importance of addressing online abuse and gender-based violence; surveillance; the need for improved digital literacy efforts; the importance of freedom of expression for discriminated people such as on the basis of sexuality; counter speech; access to critical information and education with a link to Internet access and shutdowns; were all discussed. Various stakeholders stressed the importance of a multistakeholder approach to addressing these and other challenges pertaining to human rights online.	ACCESS for: support the free flow of information while respecting applicable legal frameworks for privacy and data protection CONFIDENCE BUILDING for: ensuring the free flow of data while also protecting the integrity of that data and the privacy of individual users HUMAN RIGHTS for: addressing online gender-abuse/violence through a human rights framework
88:11	2016 - 11th IGF Chairs Summary_Final	2016	Trade Policy and the Internet which reflected the growing importance of trade issues, including domain name dispute resolution and access to registrant data, the use of encryption standards and source code disclosure mandates, and cross- borders information flows.	PRODUCT for: governments and private sector should cooperate in identifying vulnerabilities within encryption/encrypted products (and then notify developers/vendors of these issues)
89:1	2016 - Cybersecurity norms_ from articulation to implementation	2016	Reduce confict between states, lower the risk that offensive operations escalate, and prevent unacceptable consequences	CYBER STABILITY for: continuing to work towards reducing the risk of conflict stemming from ICT use STATE RESPONSIBILITY CBM: transnational consulting to reduce risk of misperception, escalation, and conflict
89:2	2016 - Cybersecurity norms_ from articulation to implementation	2016	Manage cybersecurity risk through enhanced defenses and incident response	CAPACITY BUILDING CBM: enhance capabilities to prevent and combat cybercrime by working with international entities (i.e., INTERPOL) EMERGENCY RESPONSE CBM: each state/regional partnership should establish and/or strengthen a national computer emergency response team (CERT) / cybersecurity incident response team
89:3	2016 - Cybersecurity norms_ from articulation to implementation	2016	Deliver secure products and services	PRODUCT for: developers and producers of products and services should prioritize security and stability PRODUCT for: developers and producers of products and services should take reasonable steps to ensure that their products/services are free from significant vulnerabilities
89:4	2016 - Cybersecurity norms_ from articulation to implementation	2016	UNGGE, which is the preeminent forum for development of cybersecurity norms and includes many of the leading governments as participants The United Nations Institute for Disarmament Research (UNIDIR), which has been analyzing cybersecurity and cyber norms for several years and continues to bring stakeholders from governments and the private sector together to advance cyber norms	UNITED NATIONS CBM: the United Nations (UN) may serve as an international body for decision-making, framework creation/implementation, and when developing and adopting universally agreed upon ICT norms/rules/principles (in order to ensure peace and responsible behavior/ICT use)
89:5	2016 - Cybersecurity norms_ from articulation to implementation	2016	States should not target global ICT companies to insert vulnerabilities (backdoors) or take actions that would otherwise undermine public trust in products and services	STATE RESPONSIBILITY against: targeting global ICT companies in order to insert vulnerabilities (backdoors) or take actions that would otherwise undermine public trust in products and services
89:6	2016 - Cybersecurity norms_ from articulation to implementation	2016	States should have a clear, principle- based policy for handling product and service vulnerabilities that refects a strong mandate to report them to vendors rather than to stockpile, buy, sell, or exploit them	PRODUCT for: creating transparent procedures and frameworks to asses whether and when to disclose not publicly known vulnerabilities or flaws in their information systems and/or technologies PRODUCT for: developers and producers of products and services should take measures to timely mitigate vulnerabilities that are later discovered and be transparent about their process
89:7	2016 - Cybersecurity norms_ from articulation to implementation	2016	States should commit to nonproliferation activities related to cyber weapons.	STATE RESPONSIBILITY for: commit to nonproliferation activities related to cyber weapons
89:8	2016 - Cybersecurity norms_ from articulation to implementation	2016	States should limit their engagement in cyber offensive operations to avoid creating a mass event.	STATE RESPONSIBILITY for: limiting engagement in cyber offensive operations to avoid creating a mass event/conflict
89:9	2016 - Cybersecurity norms_ from articulation to implementation	2016	States should assist private sector efforts to detect, contain, respond to, and recover from events in cyberspace.	EMERGENCY RESPONSE CBM: create procedures for mutual assistance in times of incident response
89:10	2016 - Cybersecurity norms_ from articulation to implementation	2016	Global ICT companies should not permit or enable nation-states to adversely impact the security of commercial, mass- market ICT products and services.	PRIVATE SECTOR against: permitting of enabling nation-states from adversely impacting the security of commercial, mass-market ICT products/services
89:11	2016 - Cybersecurity norms_ from articulation to implementation	2016	Global ICT companies should collaborate to proactively defend against nation- state attacks and to remediate the impact of such attacks.	PRIVATE SECTOR for: collaboration in order to proactively defend against nation-state attacks and to remediate the impact of such attacks

ID	Document	Document Groups	Quotation Content	Codes
89:12	2016 - Cybersecurity norms_ from articulation to implementation	2016	Global ICT companies should not traffc in cyber vulnerabilities for offensive purposes, nor should ICT companies embrace business models that involve proliferation of cyber vulnerabilities for offensive purposes.	PRIVATE SECTOR against: trafficking in cyber vulnerabilities for offensive purposes or embracing business models that involve proliferation of cyber vulnerabilities for offensive purposes
89:13	2016 - Cybersecurity norms_ from articulation to implementation	2016	Global ICT companies should assist public sector efforts to identify, prevent, detect, respond to, and recover from events in cyberspace	PRIVATE SECTOR for: assist public sector efforts to idenfiy, prevent, detect, respond to, and/or recover from events in cyberspace
91:1	2016 - SingaporeASEAN MOU	2016		CONFIDENCE BUILDING for: promote cooperation in regional confidence-building measures (CBMs) INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information
91:2	2016 - SingaporeASEAN MOU	2016		NORMS CBM: further dialogue regarding norms pertaining to State use of ICTs
92:1	2016 - 161020_Australia_US_Cyber_Security_Dialogue_Readout	2016	Cognisant of this and the growing importance of cybersecurity discussions, Prime Minister Malcolm Turnbull travelled to Washington DC for bilateral meetings with President Obama in January this year, ready to talk cyber security on multiple fronts.	INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information
92:2	2016 - 161020_Australia_US_Cyber_Security_Dialogue_Readout	2016	Bringing together the public and private sector with leading academic thinkers was the clear next step in growing the depth, complexity and strength of the bilateral relationship.	STAKEHOLDER COOPERATION for: encourage participation of other stakeholders such as the private sector, academia, and civil society orgs (as appropriate) for CBM and/or norm creation and implementation
92:3	2016 - 161020_Australia_US_Cyber_Security_Dialogue_Readout	2016	collaborative cyber capacity-building projects involving US and Australian governments, but perhaps more importantly, collaborating with the private sector entities who are keen to have a fair opportunity to build their digital businesses in the Asia-Pacific.	CAPACITY BUILDING CBM: encourage further work in capacity-building
95:1	2016 - 2nd Japan Australia Cyber Dialogue	2016		INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information
95:2	2016 - 2nd Japan Australia Cyber Dialogue	2016		INTERNATIONAL LAW for: applicability of international law to cyberspace NORMS CBM: further dialogue regarding norms pertaining to State use of ICTs
95:3	2016 - 2nd Japan Australia Cyber Dialogue	2016		CONFIDENCE BUILDING for: promote cooperation in regional confidence-building measures (CBMs)
95:4	2016 - 2nd Japan Australia Cyber Dialogue	2016		CRITICAL INFRASTRUCTURE for: protecting critical infrastructures
95:5	2016 - 2nd Japan Australia Cyber Dialogue	2016		EMERGENCY RESPONSE CBM: assist in strengthening cooperation amongst national computer ER teams etc. EMERGENCY RESPONSE CBM: create procedures for mutual assistance in times of incident response EMERGENCY RESPONSE CBM: each state/regional partnership should establish and/or strengthen a national computer emergency response team (CERT) / cybersecurity incident response team
95:6	2016 - 2nd Japan Australia Cyber Dialogue	2016		CAPACITY BUILDING CBM: develop regional approaches to capacity-building CAPACITY BUILDING CBM: encourage further work in capacity-building
95:7	2016 - 2nd Japan Australia Cyber Dialogue	2016		STAKEHOLDER COOPERATION for: conduct joint cybersecurity and/or related law enforcement exercises between nation states STAKEHOLDER COOPERATION for: coordinate/cooperate in combatting cybercrime
96:1	2016 - 4th JapanUS Cyber Dialogue	2016		INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information
96:2	2016 - 4th JapanUS Cyber Dialogue	2016		CRITICAL INFRASTRUCTURE for: protecting critical infrastructures
96:3	2016 - 4th JapanUS Cyber Dialogue	2016		CAPACITY BUILDING CBM: develop regional approaches to capacity-building STAKEHOLDER COOPERATION CBM: form bilateral and multilateral cooperation initiatives to build on established partnerships/relationships

ID	Document	Document Groups	Quotation Content	Codes
97:1	2016 - Singapore and Netherlands MOU	2016		INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information
97:2	2016 - Singapore and Netherlands MOU	2016		STAKEHOLDER COOPERATION CBM: form bilateral and multilateral cooperation initiatives to build on established partnerships/relationships
97:3	2016 - Singapore and Netherlands MOU	2016		INFORMATION EXCHANGE for: sharing of good/best practices in relation to ICTs and cybersecurity
97:4	2016 - Singapore and Netherlands MOU	2016		CRITICAL INFRASTRUCTURE for: protecting critical infrastructures NORM for: promote cooperation in training to develop ICT/cybersecurity awareness and skills
98:1	2016 - Singapore Strengthens Partnership with the United States	2016	Agency of Singapore (CSA), and Suzanne Spaulding, Under Secretary for the National Protection and Programs Directorate (NPPD) at the Department of Homeland Security (DHS). The signing ceremony took place at Blair House.	INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information
98:2	2016 - Singapore Strengthens Partnership with the United States	2016	CERT- CERT information exchanges and sharing of best practices,	EMERGENCY RESPONSE CBM: assist in strengthening cooperation amongst national computer ER teams etc. INFORMATION EXCHANGE for: sharing of good/best practices in relation to ICTs and cybersecurity
98:3	2016 - Singapore Strengthens Partnership with the United States	2016	coordination in cyber incident response and sharing of best practices on Critical Information Infrastructure protection	CRITICAL INFRASTRUCTURE for: protecting critical infrastructures EMERGENCY RESPONSE CBM: create procedures for mutual assistance in times of incident response
98:4	2016 - Singapore Strengthens Partnership with the United States	2016	conduct joint cybersecurity exercises and collaborate on regional cyber capacity building and cybersecurity awareness building activities	CAPACITY BUILDING CBM: assign appropriate weight to ICT security awareness and capacity building in development and assistance planning NORM for: promote cooperation in training to develop ICT/cybersecurity awareness and skills STAKEHOLDER COOPERATION for: conduct joint cybersecurity and/or related law enforcement exercises between nation states
100:1	2016 - Goa Declaration 8th BRICS Summi	2016	We, the Leaders of the Federative Republic of Brazil, the Russian Federation, the Republic of India, the People's Republic of China and the Republic of South Africa, met on 15-16 October 2016 in Goa, India, at the Eighth BRICS Summit, which was held under the theme "Building Responsive, Inclusive and Collective Solutions	INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information
100:2	2016 - Goa Declaration 8th BRICS Summi	2016	we reiterate our commitment to the principles of the Charter of the United Nations.	STATE RESPONSIBILITY for: adhering to rules and regulations agreed upon by previously enacted international law/mandates/treaties
100:3	2016 - Goa Declaration 8th BRICS Summi	2016	central role of the United Nations as the universal multilateral organisation entrusted with the mandate for maintaining international peace and security	UNITED NATIONS CBM: the United Nations (UN) may serve as an international body for decision-making, framework creation/implementation, and when developing and adopting universally agreed upon ICT norms/rules/principles (in order to ensure peace and responsible behavior/ICT use)
100:4	2016 - Goa Declaration 8th BRICS Summi	2016	including through organised crime by means of money-laundering, drug trafcking, criminal activities, dismantling terrorist bases, and countering misuse of the Internet including social media by terror entities through misuse of the latest Information and Communication Technologies (ICTs).Successfully combating terrorism requires a holistic approach. All counter- terrorism measures should uphold international law and respect human rights	CYBER ATTACKS for: strengthen tools and resources needed to prepare, deter, defend, and respond to unlawful use of ICTs, cyber attacks / acts of cyber crime and/or terrorism HUMAN RIGHTS for: applicability of international human rights law(s) to cyberspace HUMAN RIGHTS for: respecting human rights and fundamental freedoms; applying them to cyber space / ICT use, etc. INTERNATIONAL LAW for: applicability of international law to cyberspace STAKEHOLDER COOPERATION for: work / intensify cooperation against criminal/terrorist use of ICTs
100:5	2016 - Goa Declaration 8th BRICS Summi	2016	improving cooperation between our technical, law enforcement, R&D and innovation in the feld of ICTs and capacity building institutions	CAPACITY BUILDING for: taking a holistic and coordinated approach when addressing regional cybersecurity cooperation and capacity building CONFIDENCE BUILDING for: enhance trust,, confidence, and cooperation regarding ICTs, cyberspace and cybersecurity CONFIDENCE BUILDING for: promote cooperation in regional confidence-building measures (CBMs)

ID	Document	Document Groups	Quotation Content	Codes
100:6	2016 - Goa Declaration 8th BRICS Summi	2016	We afrm our commitment to bridging digital and technological divides, in particular between developed and developing countries.	ASSISTANCE CBM: provide assistance and training to developing countries to improve cybsecurity and ICT use DIGITAL EQUALITY for: closing the digital divide (i.e., by empowering communities to benefit from digital opportunities)
100:7	2016 - Goa Declaration 8th BRICS Summi	2016	quality of that access.	NORM for: promote an open, secure, stable, accessible, and peaceful cyber space / ICT environment
100:8	2016 - Goa Declaration 8th BRICS Summi	2016	We recognise that the states have the leading role to ensure stability and security in the use of ICTs	CYBER STABILITY for: maintaining a secure, safe, and trustable ICT environment
100:9	2016 - Goa Declaration 8th BRICS Summi	2016	e-governance, fnancial inclusion, and 3/2/2018 Goa Declaration at 8th BRICS Summit http://www.mea.gov.in/bilateral-documents.htm?dtl/27491/Goa+Declaration+at+8th+BRICS+Summit 13/15 targeted delivery of benefts, e-commerce, open government, digital content and services and bridging the digital divide. We support eforts aimed at capacity building for efective participation in e-commerce trade to ensure shared benefts.	CAPACITY BUILDING CBM: develop regional approaches to capacity-building DIGITAL ECONOMY for: take steps to ensure digital financial inclusion in regards to technologically enabled finances (i.e., e-commerce) STAKEHOLDER COOPERATION CBM: cooperation between states/entities (domestic and/or international) is important for furthering economic relationships/development
101:1	2016 - 1st Canada-China High-Level National Security	2016	On September 12, 2016, Wang Yongqing, Secretary-General of the Central Political and Legal Aßairs Commission of the Communist Party of China, and Daniel Jean, National Security Advisor to the Prime Minister of Canada, co-chaired in Beijing the inaugural meeting of the Canada-China High-Level National Security and Rule of Law Dialogue. The Dialogue, supported by relevant ministries and agencies of both countries, was established by Canadian and Chinese Leaders during the visit to China of Canada's Prime Minister Justin Trudeau between August 30 and September 6, 2016.	INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information
101:2	2016 - 1st Canada-China High-Level National Security	2016	ooperation on a wide range of issues including counter- terrorism; cyber security and combatting cybercrime; combatting transnational organized crime; law enforcement issues; consular issues; and judicial cooperation and exchanges on rule of law.	CYBER ATTACKS for: strengthen tools and resources needed to prepare, deter, defend, and respond to unlawful use of ICTs, cyber attacks / acts of cyber crime and/or terrorism INTERNATIONAL LAW CBM: states should publicly express their views on how existing international law applies to activities in cyberspace (in order to improve transparency, etc.)
102:1	2016 - China-UK High Level Security Dialogue	2016	On 13 June 2016, Secretary-General of the Central Commission on Political and Legal Affairs (CCPLA) Wang Yongqing and the UK National Security Adviser Mark Lyall Grant co-chaired the first China-UK High Level Security Dialogue. The two sides agreed that this first dialogue was an important measure to implement the Joint Statement on the Global Comprehensive Strategic Partnership (https://www.gov.uk/government/news/uk-china-joint- statement-2015) for the 21st Century. At the dialogue, the two sides had in-depth discussions and agreed the direction of future cooperation in counter-terrorism, cyber crime, organised crime, illegal migration and related fields. The two sides also had bilateral discussions with relevant departments. The two sides agreed to strengthen cooperation in security, law enforcement and justice issues between their two countries and to increase communication and coordination in the UN and other multilateral fora to work together against global threats according to the principle of equality and mutual trust, and sincere pragmatism	INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information STATE RESPONSIBILITY for: adhering to rules and regulations agreed upon by previously enacted international law/mandates/treaties
102:2	2016 - China-UK High Level Security Dialogue	2016	in the face of ever more serious challenges for the international community in fighting terrorism that it is in both sides' interests to develop their bilateral cooperation in counter-terrorism; in their anti-terrorism cooperation the two sides will recognise each others' concerns about major security interests and develop pragmatic cooperation to tackle terrorist threats faced in common and individually. to establish cooperation mechanisms and develop effective coordination to protect the two countries citizens, diplomatic missions and overseas economic interests. to share experiences of related measures to cut off the finances of terrorist organisations and to exchange information on legislation effected and implemented. to deepen the exchange of experience on counter-terrorism, including through a new track 2 dialogue and to work together to resolve the root causes of terrorism and extremism.	CYBER ATTACKS for: strengthen tools and resources needed to prepare, deter, defend, and respond to unlawful use of ICTs, cyber attacks / acts of cyber crime and/or terrorism
102:3	2016 - China-UK High Level Security Dialogue	2016	ot to conduct or support cyber enabled theft of intellectual property, trade secrets or confidential business information with the intent of providing commercial advantage.	STATE RESPONSIBILITY & SOVEREIGNTY against: conducting or supporting ICT-enabled theft of intellectual property, trade secrets, or other confidential business info

ID	Document	Document Groups	Quotation Content	Codes
102:4	2016 - China-UK High Level Security Dialogue	2016	to increase cooperation on cyber security related incidents and emergencies, agreeing to respond promptly to any request for information or assistance from the other participant in relation to malicious activities, in accordance with their respective national legislation and relevant international obligations. This will include, through the UK-China security dialogue, promoting information exchange and establishing a route of escalation for resolving problems.	EMERGENCY RESPONSE CBM: assist in strengthening cooperation amongst national computer ER teams etc. EMERGENCY RESPONSE CBM: create procedures for mutual assistance in times of incident response
102:5	2016 - China-UK High Level Security Dialogue	2016	cooperation in the field of law enforcement in order to prevent and combat the use of the internet to incite, recruit, finance and plan terrorist activities	STAKEHOLDER COOPERATION CBM: enhance law enforcement cooperation to reduce incidents that may be misinterpreted as hostile State actions
102:6	2016 - China-UK High Level Security Dialogue	2016	confirm that international law, in particular the UN Charter, is applicable to the use of information and communications technologies.	INTERNATIONAL LAW for: applicability of international law to cyberspace
103:1	2016 - EU-U.S. Cyber Dialogue	2016	On the occasion of the third meeting of the EU-U.S. Cyber Dialogue in Brussels on December 16, the participants jointly affirmed specific areas of cooperation as follows	INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information
103:2	2016 - EU-U.S. Cyber Dialogue	2016	at existing international law applies to state conduct in cyberspace and commit to the view that all states should abide by norms of responsible state behavior.	INTERNATIONAL LAW for: applicability of international law to cyberspace
103:3	2016 - EU-U.S. Cyber Dialogue	2016	Both sides also affirmed the importance of Confidence Building Measures (CBMs) within the Organization for Security Cooperation in Europe, welcomed the endorsement of the second set of CBMs by the Ministerial Council of the OSCE in December 2016, urged for the full implementation of the two sets of CBMs, and looked forward to the further development of CBMs in order to reinforce cooperation, build trust, and reduce the prospects for conflict in cyberspace	CONFIDENCE BUILDING for: develop and implement [practical] cyber confidence building measures (CBMs) between nation states STAKEHOLDER COOPERATION for: support other international and/or regional cooperative partnerships
103:4	2016 - EU-U.S. Cyber Dialogue	2016	Participants welcomed the continuation of the UN Group of Governmental Experts in the Field of Information and Telecommunications in the Context of International Security and its important role in identifying non-binding, peacetime norms of responsible state behavior in cyberspace and further studying how existing international law applies to state conduct in cyberspace.	UNITED NATIONS CBM: the United Nations (UN) may serve as an international body for decision-making, framework creation/implementation, and when developing and adopting universally agreed upon ICT norms/rules/principles (in order to ensure peace and responsible behavior/ICT use) UNITED NATIONS for: following the United Nation's (UN) [2015 and or 2013] GGE report's call for all States to be guided in their use of ICTs in relation to the report
103:5	2016 - EU-U.S. Cyber Dialogue	2016	exchanging views and good practices,	INFORMATION EXCHANGE for: sharing of good/best practices in relation to ICTs and cybersecurity
103:6	2016 - EU-U.S. Cyber Dialogue	2016	coordinating their respective global cyber capacity building initiatives.	CAPACITY BUILDING CBM: encourage further work in capacity-building
103:7	2016 - EU-U.S. Cyber Dialogue	2016	global multi-stakeholder community	STAKEHOLDER COOPERATION for: coordinate/cooperate in preserving multistakeholder internet governance
103:8	2016 - EU-U.S. Cyber Dialogue	2016	The European Union and the United States reaffirmed that the same rights people have offline must also be protected online, in particular freedom of expression as well as the right to be free from arbitrary and unlawful interference with privacy	INDIVIDUAL RIGHTS for: acknowledging that the same rights that individuals have offline are also protected online
103:9	2016 - EU-U.S. Cyber Dialogue	2016	promote and protect existing international human rights law	HUMAN RIGHTS for: applicability of international human rights law(s) to cyberspace
103:10	2016 - EU-U.S. Cyber Dialogue	2016	The EU and the United States affirmed their commitment to support an open and free Internet and condemned efforts by some governments or other actors to exploit the Internet to repress democratic activity and attack individuals online.	NORM for: promote an open, secure, stable, accessible, and peaceful cyber space / ICT environment
103:11	2016 - EU-U.S. Cyber Dialogue	2016	Both the European Union and the United States stressed the importance of protecting cyberspace from abuse and criminal activities for the benefit of our economies and societies, and therefore the need for law enforcement and judicial authorities to have effective tools to investigate and prosecute criminal acts related to cyberspace. Both participants affirmed their commitment to promote the Convention on Cybercrime ("Budapest Convention") in the fight against cybercrime, including by working together in international fora	CYBER ATTACKS for: strengthen tools and resources needed to prepare, deter, defend, and respond to unlawful use of ICTs, cyber attacks / acts of cyber crime and/or terrorism STATE RESPONSIBILITY for: adhering to rules and regulations agreed upon by previously enacted international law/mandates/treaties

ID	Document	Document Groups	Quotation Content	Codes
103:12	2016 - EU-U.S. Cyber Dialogue	2016	Furthermore the EU and the United States recognized the need to enhance transatlantic cooperation between civil society, academia, and the private sector to aid both societies to be appropriately defended in the face of increasing malicious cyber activity by criminals, states, proxies, and terrorist organizations. To support burgeoning governmental transatlantic cooperation in / The Office of Website Management, Bureau of Public Affairs, manages this site as a portal for information from the U.S. State Department. External links to other Internet sites should not be construed as an endorsement of the views or privacy policies contained therein. Note: documents in Portable Document Format (PDF) require Adobe Acrobat Reader 5.0 or higher to view, download Adobe Acrobat Reader (http://get.adobe.com/reader/). cyberspace, the EU and the United States launched the Transatlantic Cyber Policy Research Initiative, bringing together European and U.S. civil society, academic, industry and think-tank experts to address key cyber policy challenges and increase policy research capacity on cyber issues.	INFORMATION EXCHANGE CBM: encourage further analysis and study by research institutes and universities on ICT security related matters INFORMATION EXCHANGE CBM: encouraging exchanges between research and academic institutions
104:1	2016 - France-U.S. Cyber Bilateral Meeting	2016	This Ärst France-U.S. Cyber Bilateral Meeting strengthened the longstanding partnership between France and the United States on critical global cyber issues by reaÆrming our already effective collaboration on key cyber topics and identifying additional areas for cooperation and enhancement. The meeting represented a “whole-of-government” approach, allowing for in-depth cooperation on a wide range of cyber issues between French and American government agency counterparts and increased collaboration on both strategic and operational objectives.	INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information
104:2	2016 - France-U.S. Cyber Bilateral Meeting	2016	Strategic objectives of the meeting included aÆrming common approaches to promoting domestic and international cyber security; enhancing existing information sharing; countering use of the Internet for terrorist purposes, including radicalization and recruiting to violence online; promoting the Council of Europe Convention of Cybercrime (Budapest Convention); and pursuing cyber capacity building efforts in third countries.	STAKEHOLDER COOPERATION for: work / intensify cooperation against criminal/terrorist use of ICTs STATE RESPONSIBILITY for: adhering to rules and regulations agreed upon by previously enacted international law/mandates/treaties
104:3	2016 - France-U.S. Cyber Bilateral Meeting	2016	The meeting included discussions of international security in cyberspace focused on the current round of the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (GGE) as well as in regional security bodies, like the Organization for Security and Cooperation in Europe.	UNITED NATIONS for: following the United Nation's (UN) [2015 and or 2013] GGE report's call for all States to be guided in their use of ICTs in relation to the report
105:1	2016 - Fact Sheet for Obama Meeting with President Xi Jinping	2016	On September 3, 2016, President Barack Obama met with President Xi Jinping of China for a bilateral meeting on the margins of the G20 Leaders Summit in Hangzhou, China. The two heads of state exchanged views on a range of global, regional, and bilateral subjects. President Obama and President Xi affirmed their commitment to work together to constructively manage differences and decided to expand and deepen cooperation in the following areas:	INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information
105:2	2016 - Fact Sheet for Obama Meeting with President Xi Jinping	2016	Law Enforcement – The two sides decided to continue expanding law enforcement and anti-corruption cooperation, including by enhancing coordination and cooperation on criminal investigations and repatriations of fugitives and illegal immigrants. Both sides will continue to prioritize cooperation on repatriating fugitives and illegal immigrants through charter flights and issuance of travel documents. Counterterrorism – The United States and China condemn all forms of terrorism and decided to improve information-sharing on foreign terrorist fighters, including sharing biographical information and debriefing reports. As Permanent Members of the UN Security Council, both sides recognize the importance of reporting of foreign terrorist fighters to international databases, including Interpol. The United States and China reaffirmed their commitment to communicate and cooperate in the UN Security Council 1267 Committee to designate terrorist entities in accordance with relevant UN Security Council Resolutions.	CYBER ATTACKS for: strengthen tools and resources needed to prepare, deter, defend, and respond to unlawful use of ICTs, cyber attacks / acts of cyber crime and/or terrorism

ID	Document	Document Groups	Quotation Content	Codes
105:3	2016 - Fact Sheet for Obama Meeting with President Xi Jinping	2016	Both sides reaffirmed their intent to implement fully the September 2015 cyber commitments, including combatting malicious cyber activity and hacking, and not conducting or knowingly supporting cyber-enabled theft of intellectual property for commercial gain.	CYBER ATTACK for: preventing ICT-enabled theft of intellectual property (this includes trade secrets and other confidential business information) STAKEHOLDER COOPERATION for: coordinate/cooperate in combatting cybercrime STAKEHOLDER COOPERATION for: work with states and/or the private sector/civil society (international and/or domestic) to further cooperate on topics such as law enforcement, prosecution, investment, e-commerce, intellectual property rights, etc. STATE RESPONSIBILITY & SOVEREIGNTY against: conducting or supporting ICT-enabled theft of intellectual property, trade secrets, or other confidential business info STATE RESPONSIBILITY for: adhering to rules and regulations agreed upon by previously enacted international law/mandates/treaties
105:4	2016 - Fact Sheet for Obama Meeting with President Xi Jinping	2016	including critical infrastructure protection.	CRITICAL INFRASTRUCTURE for: protecting critical infrastructures
106:1	2016 - The 2016 G-20 Summit in Hangzhou, China	2016	President Obama participated in his 10th and final G-20 Leaders' Summit in Hangzhou, China on September 4-5. In 2009, President Obama proposed elevating the G-20 to be the world's premier forum for international economic cooperation, allowing leaders representing approximately 85 percent of global economic output to advance the shared objective of strong, sustainable, balanced, and inclusive global growth	INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information
106:2	2016 - The 2016 G-20 Summit in Hangzhou, China	2016	Free Flow of Data and Internet Governance: The G-20 endorsed a blueprint on innovative growth that affirms the importance of preserving the global nature of the internet as an engine for growth, and expressed the G-20's commitment to the free flow of information, ideas, and knowledge across borders, freedom of expression, and the multistakeholder approach to internet governance. The United States continues to promote policies around the world that support digital trade, stoke innovation, and empower and protect consumers and rejects approaches that would unduly limit growth, fragment global networks, or unfairly tilt the playing field. The United States also is working to fulfill its commitment to privatize the Internet domain name system, in cooperation with the global multistakeholder community.	ACCESS CBM: creating a free flow of and acccess to the internet is essential for the digital economy, and beneficial to development ACCESS for: support the free flow of information while respecting applicable legal frameworks for privacy and data protection CONFIDENCE BUILDING CBM: recognize importance of ICTs as the key driver of governance, economy, commerce, trade, and social well-being CONFIDENCE BUILDING for: ensuring the free flow of data while also protecting the integrity of that data and the privacy of individual users DIGITAL ECONOMY CBM: recognize the importance of the relationship between trade and the digital economy STAKEHOLDER COOPERATION for: coordinate/cooperate in preserving multistakeholder internet governance
106:3	2016 - The 2016 G-20 Summit in Hangzhou, China	2016	The G-20 reaffirmed the goal of ensuring the next 1.5 billion people are connected to the Internet by SHARE THIS: TWITTER □ FACEBOOK □ EMAIL □ 11/19/2020 FACT SHEET: The 2016 G-20 Summit in Hangzhou, China | whitehouse.gov https://obamawhitehouse.archives.gov/the-press-office/2016/09/05/fact-sheet-2016-g-20-summit-hangzhou-china 5/7 2020, a goal shared by the Global Connect Initiative led by the United States. Domestically, the United States is pursuing such policies under the Administration's ConnectED and ConnectAll initiatives.	ACCESS CBM: access to the internet is an important enabler of development./growth/innovation NORM for: promote an open, secure, stable, accessible, and peaceful cyber space / ICT environment
106:4	2016 - The 2016 G-20 Summit in Hangzhou, China	2016	Protecting Intellectual Property and Cybersecurity: The G-20 recognized the key role of effective protection and enforcement of intellectual property rights to development of the digital economy and affirmed their 2015 commitment that G-20 members should not conduct or support cyber-enabled theft of intellectual property. Building on these cyberspace commitments in Antalya, this year the G-20 committed to address security risks, threats, and vulnerabilities in the digital economy, including through application of risk-based cybersecurity approaches. The G-20's commitment echoes U.S. efforts to promote risk-based cybersecurity approaches through the President's Executive Order on Promoting Critical Infrastructure Cybersecurity and the National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity	CYBER ATTACK for: preventing ICT-enabled theft of intellectual property (this includes trade secrets and other confidential business information) STAKEHOLDER COOPERATION for: work with states and/or the private sector/civil society (international and/or domestic) to further cooperate on topics such as law enforcement, prosecution, investment, e-commerce, intellectual property rights, etc. STATE RESPONSIBILITY & SOVEREIGNTY against: conducting or supporting ICT-enabled theft of intellectual property, trade secrets, or other confidential business info

ID	Document	Document Groups	Quotation Content	Codes
107:1	2016 - G7 Principles and Actions on Cyber	2016	We affirm that the openness, interoperability, reliability, and security of the Internet have been and remain key to its development and success and that it also enhances the common values of G7, such as freedom, democracy and human rights. We reaffirm that the free flow of information is a fundamental principle to promote the global economy and development, and ensures a fair and equal access to the cyberspace for all actors of digital economy. We reaffirm the importance of respecting and promoting privacy, data protection and cyber security. We emphasize our commitment to a multi-stakeholder approach to Internet governance. We enjoy the same human rights online as well as offline, we dedicate ourselves to promoting and protecting human rights and principles of rule of law online. We emphasize the role of information and communications technologies (ICTs) in addressing global challenges and achieving progress on the 2030 Agenda for Sustainable Development.	ACCESS CBM: creating a free flow of and acccess to the internet is essential for the digital economy, and beneficial to development ACCESS for: support the free flow of information while respecting applicable legal frameworks for privacy and data protection CONFIDENCE BUILDING for: ensuring the free flow of data while also protecting the integrity of that data and the privacy of individual users INDIVIDUAL RIGHTS for: acknowledging that the same rights that individuals have offline are also protected online NORM for: promote an open, secure, stable, accessible, and peaceful cyber space / ICT environment STATE RESPONSIBILITY for: enacting cybersecurity measures that will protect people (privacy, and physical safety, etc) and inform users (transparency)
107:2	2016 - G7 Principles and Actions on Cyber	2016	We are concerned about growing uses of cyberspace for terrorist purposes such as recruitment, financing, training, operations, and incitement to violence. We affirm that international law, including the United Nations Charter, is applicable in cyberspace.	INTERNATIONAL LAW for: applicability of international law to cyberspace STAKEHOLDER COOPERATION for: work / intensify cooperation against criminal/terrorist use of ICTs STATE RESPONSIBILITY for: adhering to rules and regulations agreed upon by previously enacted international law/mandates/treaties
107:3	2016 - G7 Principles and Actions on Cyber	2016	We affirm that 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. We also recognize that 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.	HUMAN RIGHTS for: applicability of international human rights law(s) to cyberspace
107:4	2016 - G7 Principles and Actions on Cyber	2016	We commit to promote a strategic framework of international cyber stability consisting of the applicability of existing international law to state behavior in cyberspace, the promotion of voluntary norms of responsible state behavior during peacetime, and the development and the implementation of practical cyber confidence building measures between states. In this context, we welcome the report of the UN Group of Governmental Experts (GGE) in 2015 and call upon all states to be guided by the assessments and recommendations of the report.	UNITED NATIONS for: following the United Nation's (UN) [2015 and or 2013] GGE report's call for all States to be guided in their use of ICTs in relation to the report
107:5	2016 - G7 Principles and Actions on Cyber	2016	We support the continued development and implementation of cyber confidence building measures between states to promote trust and reduce the risk of conflict stemming from the	CONFIDENCE BUILDING for: develop and implement [practical] cyber confidence building measures (CBMs) between nation states
107:6	2016 - G7 Principles and Actions on Cyber	2016	We reaffirm 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.	CYBER ATTACK for: preventing ICT-enabled theft of intellectual property (this includes trade secrets and other confidential business information) STATE RESPONSIBILITY & SOVEREIGNTY against: conducting or supporting ICT-enabled theft of intellectual property, trade secrets, or other confidential business info
108:1	2016 - G7 Ise Shima Leaders' Declaration	2016	following the adoption of the 2030 Agenda for Sustainable Development (2030 Agenda) and the Paris Agreement on climate change last year, we will further make efforts to implement our commitments	STATE RESPONSIBILITY for: adhering to rules and regulations agreed upon by previously enacted international law/mandates/treaties
108:2	2016 - G7 Ise Shima Leaders' Declaration	2016	We strongly support an accessible, open, interoperable, reliable and secure cyberspace as one essential foundation for economic growth and prosperity	NORM for: promote an open, secure, stable, accessible, and peaceful cyber space / ICT environment
108:3	2016 - G7 Ise Shima Leaders' Declaration	2016	bridging digital divides,	DIGITAL EQUALITY for: closing the digital divide (i.e., by empowering communities to benefit from digital opportunities)
108:4	2016 - G7 Ise Shima Leaders' Declaration	2016	enhancing digital literacy.	EDUCATION for: increased eduation, [digital] literacy, and awareness regarding digital rights and ways to exercise/protect them
108:5	2016 - G7 Ise Shima Leaders' Declaration	2016	democracy and respect for privacy and human rights	HUMAN RIGHTS for: respecting human rights and fundamental freedoms; applying them to cyber space / ICT use, etc.
108:6	2016 - G7 Ise Shima Leaders' Declaration	2016	international law is applicable in cyberspace	INTERNATIONAL LAW for: applicability of international law to cyberspace
108:7	2016 - G7 Ise Shima Leaders' Declaration	2016	the promotion of voluntary norms of responsible state behavior during peacetime, and the development and the implementation of practical cyber confidence building measures between states. I	CONFIDENCE BUILDING for: develop and implement [practical] cyber confidence building measures (CBMs) between nation states NORMS CBM: universally agreed upon [voluntary] norms/rules/principles are important for the responsible behavior of States' use of ICTs

ID	Document	Document Groups	Quotation Content	Codes
108:8	2016 - G7 Ise Shima Leaders' Declaration	2016	In this context, we welcome the report of the UN Group of Governmental Experts in 2015 and call upon all states to be guided by the assessments and recommendations of the report	UNITED NATIONS for: following the United Nation's (UN) [2015 and or 2013] GGE report's call for all States to be guided in their use of ICTs in relation to the report
108:9	2016 - G7 Ise Shima Leaders' Declaration	2016	We also reaffirm that no country 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 its companies or commercial sectors	CYBER ATTACK for: preventing ICT-enabled theft of intellectual property (this includes trade secrets and other confidential business information) STATE RESPONSIBILITY & SOVEREIGNTY against: conducting or supporting ICT-enabled theft of intellectual property, trade secrets, or other confidential business info
108:10	2016 - G7 Ise Shima Leaders' Declaration	2016	We commit to facilitate the free flow of information to ensure openness, transparency and freedom of the Internet, and a fair and equal access to the cyberspace for all actors of digital economy while respecting privacy and data protection, as well as cyber security	ACCESS for: support the free flow of information while respecting applicable legal frameworks for privacy and data protection CONFIDENCE BUILDING for: ensuring the free flow of data while also protecting the integrity of that data and the privacy of individual users
108:11	2016 - G7 Ise Shima Leaders' Declaration	2016	We commit to promote a multi-stakeholder approach to Internet governance which includes full and active participation by governments, the private sector, civil society, the technical community, and international organizations, among others	STAKEHOLDER COOPERATION for: coordinate/cooperate in preserving multistakeholder internet governance STAKEHOLDER COOPERATION for: encourage participation of other stakeholders such as the private sector, academia, and civil society orgs (as appropriate) for CBM and/or norm creation and implementation
109:1	2016 - CICTE OAS session	2016	THE MEMBER STATES OF THE INTER-AMERICAN COMMITTEE AGAINST TERRORISM (CICTE) of the Organization of American States (OAS), meeting at its sixteenth regular session, held in Washington, D.C., in the United States of America, on February 25 and 26, 2016:	INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information
109:2	2016 - CICTE OAS session	2016	ALSO REAFFIRMING resolution AG/RES. 1939 (XXXIII-0/03), "Development of an Inter-American Strategy to Combat Threats to Cybersecurity," and reaffirming resolution AG/RES. 2004 (XXXIV-0/04), "Adoption of a Comprehensive Inter- American Strategy to Combat Threats to Cybersecurity: A Multidimensional and Multidisciplinary Approach to Creating a Culture of Cybersecurity"	STATE RESPONSIBILITY for: adhering to rules and regulations agreed upon by previously enacted international law/mandates/treaties
109:3	2016 - CICTE OAS session	2016	fighting against cyber threats and cybercrime, criminilazing attacks against cyberspace, protecting critical infrastructure and securing networked systems	CRITICAL INFRASTRUCTURE for: protecting critical infrastructures CYBER ATTACKS for: strengthen tools and resources needed to prepare, deter, defend, and respond to unlawful use of ICTs, cyber attacks / acts of cyber crime and/or terrorism STAKEHOLDER COOPERATION for: work / intensify cooperation against criminal/terrorist use of ICTs
109:4	2016 - CICTE OAS session	2016	free expression and the free flow of information, exercised in accordance with member states' applicable obligations and commitments within the framework of international and regional human rights instruments, are essential for innovation and for the operation of the computer networks that underpin economic growth and social development;	ACCESS CBM: creating a free flow of and acccess to the internet is essential for the digital economy, and beneficial to development ACCESS for: support the free flow of information while respecting applicable legal frameworks for privacy and data protection CONFIDENCE BUILDING for: ensuring the free flow of data while also protecting the integrity of that data and the privacy of individual users HUMAN RIGHTS for: respecting human rights and fundamental freedoms; applying them to cyber space / ICT use, etc.
109:5	2016 - CICTE OAS session	2016	RECOGNIZING the work carried out by the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, and taking note of the reports prepared by that group (2010, 2013, 2015);	UNITED NATIONS for: following the United Nation's (UN) [2015 and or 2013] GGE report's call for all States to be guided in their use of ICTs in relation to the report
109:6	2016 - CICTE OAS session	2016	CONSIDERING the importance of member states cooperating with key stakeholders in the use of cyberspace, such as the private sector, civil society, academia, the technical community, among other stakeholders and international organizations;	STAKEHOLDER COOPERATION for: encourage participation of other stakeholders such as the private sector, academia, and civil society orgs (as appropriate) for CBM and/or norm creation and implementation
109:7	2016 - CICTE OAS session	2016	The need to establish procedures for mutual assistance when responding to incidents, in addressing short-term network security problems, and provide collaboration with the reciprocal requests made by the member countries in order to investigate and prosecute crime related to terrorist acts, including procedures for expediting that assistance;	EMERGENCY RESPONSE CBM: create procedures for mutual assistance in times of incident response
110:1	2016 - Warsaw+Summit+Communiqué +7-9-2016	2016	We, the Heads of State and Government of the member countries of the North Atlantic Alliance, have gathered in Warsaw at a deÒning moment for the security of our nations and populations. We are pleased to have been joined by Montenegro, which we have invited to become the 29th member of our Alliance.	INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information

ID	Document	Document Groups	Quotation Content	Codes
110:2	2016 - Warsaw+Summit+Communiqué +7-9-2016	2016	. We are united in our commitment to the Washington Treaty, the purposes and principles of the Charter of the United Nations (UN)	STATE RESPONSIBILITY for: adhering to rules and regulations agreed upon by previously enacted international law/mandates/treaties
110:3	2016 - Warsaw+Summit+Communiqué +7-9-2016	2016	We reaÕrm our commitment to act in accordance with international law, including the UN Charter, international humanitarian law, and human rights law, as applicable. We will continue to follow the principle of restraint and support maintaining international peace, security, and stability in cyberspace. We welcome the work on voluntary international norms of responsible state behaviour and conÒdence-building measures regarding cyberspace	HUMAN RIGHTS for: applicability of international human rights law(s) to cyberspace INTERNATIONAL LAW for: applicability of international law to cyberspace NORMS CBM: universally agreed upon [voluntary] norms/rules/principles are important for the responsible behavior of States' use of ICTs
110:4	2016 - Warsaw+Summit+Communiqué +7-9-2016	2016	Strong partnerships play a key role in e×ectively addressing cyber challenges. We will continue to deepen cooperation with the EU, as agreed, including through the on-going implementation of the Technical Arrangement that contributes to better prevention and response to cyber attacks. We will further enhance our partnerships with other international organisations and partner nations, as well as with industry and academia through the NATO Industry Cyber Partnership	STAKEHOLDER COOPERATION CBM: form bilateral and multilateral cooperation initiatives to build on established partnerships/relationships STAKEHOLDER COOPERATION for: support other international and/or regional cooperative partnerships
111:1	2016 - NATO+Cyber+Defence+Pledge +7-8-2016	2016	We reaÕrm 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 will ensure that strong and resilient cyber defences enable the Alliance to fulÒl its core tasks. Our interconnectedness means that we are only as strong as our weakest link. We will work together to better protect our networks and thereby contribute to the success of Allied operations.	CRITICAL INFRASTRUCTURE for: promoting resilience (as related to ICTs,cybersecurity, and related critical infrastructure STATE RESPONSIBILITY for: adhering to rules and regulations agreed upon by previously enacted international law/mandates/treaties
111:2	2016 - NATO+Cyber+Defence+Pledge +7-8-2016	2016	We reaÕrm the applicability of international law in cyberspace and acknowledge the work done in relevant international organisations, including on voluntary norms of responsible state behaviour and conÒdence-building measures in cyberspace	CONFIDENCE BUILDING CBM: CBM are important for increasing transparency, predictability, and stability INTERNATIONAL LAW for: applicability of international law to cyberspace NORMS CBM: universally agreed upon [voluntary] norms/rules/principles are important for the responsible behavior of States' use of ICTs
111:3	2016 - NATO+Cyber+Defence+Pledge +7-8-2016	2016	multinational projects, education, training, and exercises and information exchange	ASSISTANCE CBM: provide assistance and training to developing countries to improve cybsecurity and ICT use EDUCATION for: include cybersecurity courses in school curricula (i.e., primary school, degree courses in undergrad, professional education, and trainings INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information NORM for: promote cooperation in training to develop ICT/cybersecurity awareness and skills
112:1	2016 - Joint Statement on Third Annual Nordic-Baltic + U.S. Cyber Consultations	2016	Representatives of the Governments of Denmark, Estonia, Finland, Iceland, Latvia, Lithuania, Norway, Sweden, and the United States met in Vilnius on September 13-14, 2016 for the third annual High-level Cybersecurity Roundtable.	INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information
112:2	2016 - Joint Statement on Third Annual Nordic-Baltic + U.S. Cyber Consultations	2016	he application of international law and norms in cyberspace,	INTERNATIONAL LAW for: applicability of international law to cyberspace
112:3	2016 - Joint Statement on Third Annual Nordic-Baltic + U.S. Cyber Consultations	2016	They further acknowledged that in cyberspace, just as elsewhere, states have a special responsibility to promote security, stability, human rights, and economic ties with other nations	HUMAN RIGHTS for: applicability of international human rights law(s) to cyberspace NORM for: supporting a free and secure internet / cyber space that supports economic growth and innovation
112:4	2016 - Joint Statement on Third Annual Nordic-Baltic + U.S. Cyber Consultations	2016	. In support of those objectives, they affirmed that no state should conduct or knowingly support cyber-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.	STATE RESPONSIBILITY & SOVEREIGNTY against: conducting or supporting ICT-enabled theft of intellectual property, trade secrets, or other confidential business info

ID	Document	Document Groups	Quotation Content	Codes
112:5	2016 - Joint Statement on Third Annual Nordic-Baltic + U.S. Cyber Consultations	2016	They also endorsed the 2015 report of the UN Group of Governmental Experts in the Field of Information and Telecommunications in the Context of International Security, affirmed that existing international law applies to state conduct in cyberspace, and committed themselves to the view that all states should abide by voluntary and non-binding peacetime norms of responsible state behavior in cyberspace.	UNITED NATIONS for: following the United Nation's (UN) [2015 and or 2013] GGE report's call for all States to be guided in their use of ICTs in relation to the report
112:6	2016 - Joint Statement on Third Annual Nordic-Baltic + U.S. Cyber Consultations	2016	the principle that individuals have the same human rights online and offline	INDIVIDUAL RIGHTS for: acknowledging that the same rights that individuals have offline are also protected online
112:7	2016 - Joint Statement on Third Annual Nordic-Baltic + U.S. Cyber Consultations	2016	multistakeholder Internet governance structures that are inclusive, transparent, accountable, and technically sound; emphasized the value of the Internet Governance Forum (IGF) as the premier, global, multistakeholder forum for dialogue on Internet public policy issues; and welcomed the 10-year renewal of the IGF mandate in the UN General Assembly's 10 year review of the World Summit on the Information Society.	STAKEHOLDER COOPERATION for: coordinate/cooperate in preserving multistakeholder internet governance STAKEHOLDER COOPERATION for: support other international and/or regional cooperative partnerships
113:1	2016 - Joint+Declaration+on+the+United+States,+Estonia,+Latvia,+and+Lithuania	2016	As affirmed at the NATO Summit in Warsaw, the greatest responsibility of the Alliance is to protect and defend our territory and populations, as reflected in Article 5 of the Washington Treaty. NATO has responded to the changed security environment by enhancing its deterrence and defense posture, including through a forward presence in the eastern part of the Alliance. The Baltic States appreciate these steps by NATO, as well as the significant and visible U.S. presence in the region, which has demonstrated our collective solidarity and resolve to protect all Allies.	STATE RESPONSIBILITY for: adhering to rules and regulations agreed upon by previously enacted international law/mandates/treaties
113:2	2016 - Joint+Declaration+on+the+United+States,+Estonia,+Latvia,+and+Lithuania	2016	On the occasion of Vice President Biden's visit to Latvia, we, the United States of America, Estonia, Latvia, and Lithuania, reaffirm our strategic alliance. Faced with an unpredictable security environment, we commit to deepening our cooperation and our efforts to ensure security and stability in the region, as part of NATO's approach to collective defense	INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information
113:3	2016 - Joint+Declaration+on+the+United+States,+Estonia,+Latvia,+and+Lithuania	2016	enhancing protection of critical infrastructure	CRITICAL INFRASTRUCTURE for: protecting critical infrastructures
113:4	2016 - Joint+Declaration+on+the+United+States,+Estonia,+Latvia,+and+Lithuania	2016	This cooperation is intended to strengthen NATO and promote regional cooperation, stability, and security	CAPACITY BUILDING CBM: develop regional approaches to capacity-building CONFIDENCE BUILDING for: promote cooperation in regional confidence-building measures (CBMs) STAKEHOLDER COOPERATION for: support other international and/or regional cooperative partnerships
114:1	2016 - Fact+Sheet+United+StatesNorth+American+Leaders'+Summit	2016	Today President Obama met in Ottawa, Canada with Prime Minister Justin Trudeau of Canada and President Enrique Peña Nieto of Mexico for the North American Leaders' Summ	INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information
114:2	2016 - Fact+Sheet+United+StatesNorth+American+Leaders'+Summit	2016	affirmed the importance of an open, interoperable, reliable, and secure Internet, underpinned by the multi-stakeholder model of Internet governance	NORM for: promote an open, secure, stable, accessible, and peaceful cyber space / ICT environment STAKEHOLDER COOPERATION for: coordinate/cooperate in preserving multistakeholder internet governance
114:3	2016 - Fact+Sheet+United+StatesNorth+American+Leaders'+Summit	2016	promote stability in cyberspace by affirming the applicability of international law to state conduct in cyberspace, promoting voluntary norms of responsible state behavior during peacetime, and supporting confidence building measures between states	CONFIDENCE BUILDING CBM: promote the use of ICTs for peaceful purposes CONFIDENCE BUILDING for: develop and implement [practical] cyber confidence building measures (CBMs) between nation states INTERNATIONAL LAW for: applicability of international law to cyberspace NORMS CBM: universally agreed upon [voluntary] norms/rules/principles are important for the responsible behavior of States' use of ICTs
114:4	2016 - Fact+Sheet+United+StatesNorth+American+Leaders'+Summit	2016	Leaders affirm that no country should conduct or knowingly support online activity that intentionally damages critical infrastructure or otherwise impairs the use of critical infrastructure to provide services to the public	CRITICAL INFRASTRUCTURE against: knowingly support cyberactivity that intentionally damages or impairs the use and operation of critical infrastructure

ID	Document	Document Groups	Quotation Content	Codes
114:5	2016 - Fact+Sheet+United+StatesNorth+American+Leaders'+Summit	2016	hat no country should conduct or knowingly support activity intended to prevent national computer security incident response teams (CSIRTs) from responding to cyber incidents, or use CSIRTs to enable online activity that is intended to do harm;	CYBER ATTACKS against: states using authorized emergency response teams to engage in malicuous / harmful international activity CYBER ATTACKS against: targeting emergency response teams
114:6	2016 - Fact+Sheet+United+StatesNorth+American+Leaders'+Summit	2016	every country should cooperate, consistent with its domestic law and international	DOMESTIC LAW for: applicability of domestic law to cyber space / ICT usage
114:7	2016 - Fact+Sheet+United+StatesNorth+American+Leaders'+Summit	2016	requests for assistance from other states in mitigating malicious cyber activity emanating from its territory	CYBER ATTACKS for: responding to requests for help in the event of a cyber attack
114:8	2016 - Fact+Sheet+United+StatesNorth+American+Leaders'+Summit	2016	no country should conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to its companies or commercial sectors.	CYBER ATTACK for: preventing ICT-enabled theft of intellectual property (this includes trade secrets and other confidential business information) STAKEHOLDER COOPERATION for: work with states and/or the private sector/civil society (international and/or domestic) to further cooperate on topics such as law enforcement, prosecution, investment, e-commerce, intellectual property rights, etc. STATE RESPONSIBILITY & SOVEREIGNTY against: conducting or supporting ICT-enabled theft of intellectual property, trade secrets, or other confidential business info
114:9	2016 - Fact+Sheet+United+StatesNorth+American+Leaders'+Summit	2016	The United States, Canada, and Mexico will work together in the 2016/2017 UN Group of Governmental Experts, the Group of 20, and the Organization of American States in support of these objectives.	UNITED NATIONS for: following the United Nation's (UN) [2015 and or 2013] GGE report's call for all States to be guided in their use of ICTs in relation to the report
115:1	2016 - Nuclear+Security+Summit+Joint+Statement+on+Cyber+Security	2016	good practice	INFORMATION EXCHANGE for: sharing of good/best practices in relation to ICTs and cybersecurity
116:1	2016 - OSCE	2016	international law, including, inter alia, the UN Charter and the International Covenant on Civil and Political Rights; as well as the Helsinki Final Act; and their responsibilities to respect human rights and fundamental freedoms.	HUMAN RIGHTS for: applicability of international human rights law(s) to cyberspace HUMAN RIGHTS for: respecting human rights and fundamental freedoms; applying them to cyber space / ICT use, etc. INTERNATIONAL LAW for: applicability of international law to cyberspace STATE RESPONSIBILITY for: adhering to rules and regulations agreed upon by previously enacted international law/mandates/treaties
116:2	2016 - OSCE	2016	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.	INFORMATION EXCHANGE CBM: exchange national views on the use of ICTS in conflicts
116:3	2016 - OSCE	2016	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.	INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information STAKEHOLDER COOPERATION for: support other international and/or regional cooperative partnerships
116:4	2016 - OSCE	2016	protect critical national and international ICT infrastructures including their integrity.	CRITICAL INFRASTRUCTURE for: protecting critical infrastructures
116:5	2016 - OSCE	2016	Participating States will, on a voluntary basis, conduct activities for officials and experts to support the facilitation of authorized and protected communication channels to prevent and reduce the risks of misperception, escalation, and conflict; and to clarify technical, legal and diplomatic mechanisms to address ICT-related requests. This does not exclude the use of the channels of communication mentioned in Permanent Council Decision No. 1106.	STATE RESPONSIBILITY CBM: transnational consulting to reduce risk of misperception, escalation, and conflict

ID	Document	Document Groups	Quotation Content	Codes
116:6	2016 - OSCE	2016	Participating States will, on a voluntary basis and consistent with national legislation, promote public-private partnerships and develop mechanisms to exchange best practices of responses to common security challenges stemming from the use of ICTs.	INFORMATION EXCHANGE for: sharing of good/best practices in relation to ICTs and cybersecurity
117:1	2016 - Second U.S.-China Cybercrime High Level Joint Dialogue	2016	Today, Chinese State Councilor and Minister of Ministry of Public Security Guo Shengkun co-chaired the second U.S.- China Cybercrime and Related Issues High Level Joint Dialogue with representatives of the U.S. Departments of Justice and Homeland Security. The dialogue aims to implement the consensus reached between Chinese President Xi Jinping and U.S. President Barack Obama in September 2015 during President Xi's visit to the United States, and to enhance pragmatic bilateral cooperation with regard to cybercrime, network protection and other related issues.	INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information
117:2	2016 - Second U.S.-China Cybercrime High Level Joint Dialogue	2016	Both sides continue to develop cooperation on combating cybercrime and network protection investigations and information exchanges, aiming to conduct routine exchanges and improve cyber security cooperation.	CYBER ATTACKS for: strengthen tools and resources needed to prepare, deter, defend, and respond to unlawful use of ICTs, cyber attacks / acts of cyber crime and/or terrorism
118:1	2016 - Third+U.S.-China+High-Level+Dialogue+on+Cybercrime	2016	1. Combatting Cybercrime and Cyber-Enabled Crime. Both sides re-commit to cooperate on the investigation of cyber crimes and malicious cyber activities emanating from China or the United States and to refrain from cyber- enabled theft of intellectual property with the intent of providing competitive advantages to companies or commercial sectors. To that end, both sides: Plan to continue the mechanism of the "Status Report on U.S./China Cybercrime Cases" to evaluate the effectiveness of case cooperation. Affirm that both sides intend to focus cooperation on hacking and cyber-enabled fraud cases, share cybercrime- related leads and information with each other in a timely manner, and determine priority cases for continued law enforcement cooperation. Both sides intend to continue cooperation on cases involving online distribution of child pornography. Both sides seek to expand cyber-enabled crime cooperation to counter Darkweb marketplaces' illicit sale of synthetic drugs and firearms. Seek to provide concrete and timely updates on cases brought within the ambit of the dialogue. Exchanged views on existing channels of multilateral cooperation, and intend to continue exchanges regarding this topic.	INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information STAKEHOLDER COOPERATION for: work / intensify cooperation against criminal/terrorist use of ICTs
118:2	2016 - Third+U.S.-China+High-Level+Dialogue+on+Cybercrime	2016	, and decided to continue cooperation on information sharing in countering the use of the Internet for terrorist and other criminal purposes. Both sides will consider holding a second seminar in 2017.	STAKEHOLDER COOPERATION for: work / intensify cooperation against criminal/terrorist use of ICTs
119:1	2016 - Joint+Statement+on+U.S.-Germany+Cyber	2016	The Governments of the United States and Germany held a Cyber Bilateral Meeting in Washington, DC, on March 22- 23, 2016.	INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information
119:2	2016 - Joint+Statement+on+U.S.-Germany+Cyber	2016	Strategic objectives include affirming common approaches to promoting international cyber security, multistakeholder Internet governance, Internet freedom and the promotion of human rights online; partnering with the private sector to protect critical infrastructure; and pursuing cyber capacity building efforts in third countries.	HUMAN RIGHTS for: applicability of international human rights law(s) to cyberspace HUMAN RIGHTS for: respecting human rights and fundamental freedoms; applying them to cyber space / ICT use, etc. STAKEHOLDER COOPERATION for: coordinate/cooperate in preserving multistakeholder internet governance STAKEHOLDER COOPERATION for: work with states and/or the private sector/civil society (international and/or domestic) to further cooperate on topics such as law enforcement, prosecution, investment, e-commerce, intellectual property rights, etc.
119:3	2016 - Joint+Statement+on+U.S.-Germany+Cyber	2016	international law applies to cyberspace, the promotion of cyber norms of responsible state behavior, and the implementation of confidence building measures.	CONFIDENCE BUILDING for: develop and implement [practical] cyber confidence building measures (CBMs) between nation states INTERNATIONAL LAW for: applicability of international law to cyberspace NORMS CBM: universally agreed upon [voluntary] norms/rules/principles are important for the responsible behavior of States' use of ICTs

ID	Document	Document Groups	Quotation Content	Codes
119:4	2016 - Joint+Statement+on+U.S.-Germany+Cyber	2016	The United States and Germany welcomed the consensus 2015 UN (United Nations) Group of Governmental Experts (GGE) report affirming the applicability of international law and outlining norms of responsible state behavior in cyberspace.	UNITED NATIONS for: following the United Nation's (UN) [2015 and or 2013] GGE report's call for all States to be guided in their use of ICTs in relation to the report
119:5	2016 - Joint+Statement+on+U.S.-Germany+Cyber	2016	They will continue their close cooperation on these issues in bilateral, regional, and multilateral fora, especially as the next GGE is poised to start its work.	STAKEHOLDER COOPERATION CBM: form bilateral and multilateral cooperation initiatives to build on established partnerships/relationships STAKEHOLDER COOPERATION CBM: states should participate and cooperate in multilateral forums
119:6	2016 - Joint+Statement+on+U.S.-Germany+Cyber	2016	Both sides underscore their conviction that the same rights that people have offline must also be protected online. These include the right to seek, receive, and impart information, the freedoms of expression, peaceful assembly and association, and the right to be free from arbitrary or unlawful interference with privacy	INDIVIDUAL RIGHTS for: acknowledging that the same rights that individuals have offline are also protected online
120:1	2016 - U.S.-India+Cyber+Relationship	2016	A commitment to an open, interoperable, secure, and reliable cyberspace environment;	NORM for: promote an open, secure, stable, accessible, and peaceful cyber space / ICT environment
120:2	2016 - U.S.-India+Cyber+Relationship	2016	A commitment to promote the Internet as an engine for innovation, economic growth, and trade and commerce; A commitment to promote the free Äow of information;	NORM for: supporting a free and secure internet / cyber space that supports economic growth and innovation
120:3	2016 - U.S.-India+Cyber+Relationship	2016	A commitment to promote cooperation between and among the private sector and government authorities on cybercrime and cybersecurity;	STAKEHOLDER COOPERATION for: work with states and/or the private sector/civil society (international and/or domestic) to further cooperate on topics such as law enforcement, prosecution, investment, e-commerce, intellectual property rights, etc.
120:4	2016 - U.S.-India+Cyber+Relationship	2016	A recognition of the importance of bilateral and international cooperation for combating cyber threats and promoting cybersecurity;	STAKEHOLDER COOPERATION CBM: form bilateral and multilateral cooperation initiatives to build on established partnerships/relationships STAKEHOLDER COOPERATION CBM: states should participate and cooperate in multilateral forums
120:5	2016 - U.S.-India+Cyber+Relationship	2016	A commitment to promote international security and stability in cyberspace through a framework that recognizes the applicability of international law, in particular the UN Charter, to state conduct in cyberspace, and the promotion of voluntary norms of responsible state behavior in cyberspace during peacetime;	INTERNATIONAL LAW for: applicability of international law to cyberspace STATE RESPONSIBILITY for: adhering to rules and regulations agreed upon by previously enacted international law/mandates/treaties
120:6	2016 - U.S.-India+Cyber+Relationship	2016	A commitment to the multistakeholder model of Internet governance that is transparent and accountable to its stakeholders, including governments, civil society and the private sector, and promotes cooperation among them;	STAKEHOLDER COOPERATION for: coordinate/cooperate in preserving multistakeholder internet governance
120:7	2016 - U.S.-India+Cyber+Relationship	2016	A commitment to promote closer cooperation among law enforcement agencies to combat cybercrime between the two countries;	STAKEHOLDER COOPERATION CBM: enhance law enforcement cooperation to reduce incidents that may be misinterpreted as hostile State actions
120:8	2016 - U.S.-India+Cyber+Relationship	2016	A commitment to promote, protect, and respect human rights and fundamental freedoms online;	HUMAN RIGHTS for: applicability of international human rights law(s) to cyberspace
120:9	2016 - U.S.-India+Cyber+Relationship	2016	A desire to cooperate in strengthening the security and resilience of critical information infrastructure	CRITICAL INFRASTRUCTURE for: protecting critical infrastructures
120:10	2016 - U.S.-India+Cyber+Relationship	2016	Identifying, coordinating, sharing, and implementing cybersecurity best practices;	INFORMATION EXCHANGE for: sharing of good/best practices in relation to ICTs and cybersecurity
120:11	2016 - U.S.-India+Cyber+Relationship	2016	Sharing information on a real time or near real time basis, when practical and consistent with existing bilateral arrangements, about malicious	STATE RESPONSIBILITY for: timely responses to requests for information
120:12	2016 - U.S.-India+Cyber+Relationship	2016	Promoting voluntary norms of responsible state behavior in peacetime, including the norms identiÄed by the UN Group of Governmental Experts in the Field of Information and Telecommunications in the Context of International Security	UNITED NATIONS CBM: the United Nations (UN) may serve as an international body for decision-making, framework creation/implementation, and when developing and adopting universally agreed upon ICT norms/rules/principles (in order to ensure peace and responsible behavior/ICT use) UNITED NATIONS for: following the United Nation's (UN) [2015 and or 2013] GGE report's call for all States to be guided in their use of ICTs in relation to the report
120:13	2016 - U.S.-India+Cyber+Relationship	2016	A state should not conduct or knowingly support activity intended to prevent national Computer Security Incident Response Teams (CSIRTs) from responding to cyber incidents. States should also not use CSIRTs to enable online activity that is intended to do harm	CYBER ATTACKS against: states using authorized emergency response teams to engage in malicuous / harmful international activity CYBER ATTACKS against: targeting emergency response teams
120:14	2016 - U.S.-India+Cyber+Relationship	2016	Improving the capacity of law enforcement agencies through joint training programs, including equipping them to draft appropriate requests for electronic evidence in accordance with the respective laws and regulations of the United States and India;	STAKEHOLDER COOPERATION for: conduct joint cybersecurity and/or related law enforcement exercises between nation states

ID	Document	Document Groups	Quotation Content	Codes
120:15	2016 - U.S.-India+Cyber+Relationship	2016	A state should not conduct or knowingly support ICT-enabled theft of intellectual property, including trade secrets or other conÄdential business information, with the intent of providing competitive advantages to companies or commercial sectors;	CYBER ATTACK for: preventing ICT-enabled theft of intellectual property (this includes trade secrets and other confidential business information) STAKEHOLDER COOPERATION for: work with states and/or the private sector/civil society (international and/or domestic) to further cooperate on topics such as law enforcement, prosecution, investment, e-commerce, intellectual property rights, etc. STATE RESPONSIBILITY & SOVEREIGNTY against: conducting or supporting ICT-enabled theft of intellectual property, trade secrets, or other confidential business info
120:16	2016 - U.S.-India+Cyber+Relationship	2016	Supporting the multistakeholder model of Internet governance;	STAKEHOLDER COOPERATION for: coordinate/cooperate in preserving multistakeholder internet governance
121:1	2016 - The+U.S.+and+India+Enduring+Global+Partners	2016	cyberspace enables economic growth and development, and reaffirmed their commitment to an open, interoperable, secure, and reliable Internet, underpinned by the multistakeholder model of Internet governance	NORM for: promote an open, secure, stable, accessible, and peaceful cyber space / ICT environment NORM for: supporting a free and secure internet / cyber space that supports economic growth and innovation STAKEHOLDER COOPERATION for: coordinate/cooperate in preserving multistakeholder internet governance
121:2	2016 - The+U.S.+and+India+Enduring+Global+Partners	2016	They committed to deepen cooperation on cybersecurity and welcomed the understanding reached to finalize the Framework for the U.S.-India Cyber Relationship in the near term	STATE RESPONSIBILITY for: adhering to rules and regulations agreed upon by previously enacted international law/mandates/treaties
121:3	2016 - The+U.S.+and+India+Enduring+Global+Partners	2016	They committed to enhance cyber collaboration on critical infrastructure, cybercrime, and malicious cyber activity by state and non-state actors, capacity building, and cybersecurity research and development, and to continue discussions on all aspects of trade in technology and related services, including market access.	CAPACITY BUILDING CBM: encourage further work in capacity-building CONFIDENCE BUILDING CBM: further investments in ICT research and development CRITICAL INFRASTRUCTURE for: protecting critical infrastructures
121:4	2016 - The+U.S.+and+India+Enduring+Global+Partners	2016	They have committed to continue dialogue and engagement in Internet governance fora, including in ICANN, IGF and other venues, and to support active participation by all stakeholders of the two countries in these fora.	STAKEHOLDER COOPERATION for: support other international and/or regional cooperative partnerships
121:5	2016 - The+U.S.+and+India+Enduring+Global+Partners	2016	promotion of voluntary norms of responsible state behavior during peacetime, and the development and implementation of practical confidence building measures between states.	CONFIDENCE BUILDING for: develop and implement [practical] cyber confidence building measures (CBMs) between nation states NORMS CBM: universally agreed upon [voluntary] norms/rules/principles are important for the responsible behavior of States' use of ICTs
121:6	2016 - The+U.S.+and+India+Enduring+Global+Partners	2016	In this context, they affirmed their commitment to the voluntary norms that no country should conduct or knowingly support online activity that intentionally damages critical infrastructure or otherwise impairs the use of it to provide services to the public	CRITICAL INFRASTRUCTURE against: knowingly damaging critical infrastructure
121:7	2016 - The+U.S.+and+India+Enduring+Global+Partners	2016	security incident response teams from responding to cyber incidents, or use its own teams to enable online activity that is intended to do harm;	CYBER ATTACKS against: states using authorized emergency response teams to engage in malicuous / harmful international activity CYBER ATTACKS against: targeting emergency response teams
121:8	2016 - The+U.S.+and+India+Enduring+Global+Partners	2016	its domestic law and international obligations,	DOMESTIC LAW for: applicability of domestic law to cyber space / ICT usage INTERNATIONAL LAW for: applicability of international law to cyberspace
121:9	2016 - The+U.S.+and+India+Enduring+Global+Partners	2016	requests for assistance from other states in mitigating malicious cyber activity emanating from its territory	CYBER ATTACKS for: responding to requests for help in the event of a cyber attack STATE RESPONSIBILITY & SOVEREIGNTY for: ensuring that one's territory is not used by non-State actors to commit internationally wrongful acts using ICTs

ID	Document	Document Groups	Quotation Content	Codes
121:10	2016 - The+U.S.+and+India+Enduring +Global+Partners	2016	no country 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 its companies or commercial sectors	CYBER ATTACK for: preventing ICT-enabled theft of intellectual property (this includes trade secrets and other confidential business information) STAKEHOLDER COOPERATION for: work with states and/or the private sector/civil society (international and/or domestic) to further cooperate on topics such as law enforcement, prosecution, investment, e-commerce, intellectual property rights, etc. STATE RESPONSIBILITY & SOVEREIGNTY against: conducting or supporting ICT-enabled theft of intellectual property, trade secrets, or other confidential business info
122:1	2016 - Japan-US-ROK Experts Meeting on Cybersecurity	2016	On December 19, 2016 (EST), the Japan-US-ROK trilateral experts meeting on cybersecurity of critical infrastructure was held in Washington D.C. to enhance concrete cooperation among the three countries in the field of cyber, based on the discussion of the Japan-US-ROK Vice Minister-level meeting.	INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information STAKEHOLDER COOPERATION CBM: form bilateral and multilateral cooperation initiatives to build on established partnerships/relationships STAKEHOLDER COOPERATION CBM: states should participate and cooperate in multilateral forums
123:1	2016 - UK-U.S.+Cyber+Agreement+9-8-2016	2016	British counterpart Michael Fallon yesterday signed a first-of-its kind agreement to together advance offensive and defensive cyber capabilities, Carter said in a joint press conference in London as part of his three-day trip to the United Kingdom and Norway	INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information
123:2	2016 - UK-U.S.+Cyber+Agreement+9-8-2016	2016	information and perform vital research and development together to advance their offensive and defensive cyber capabilities as the	CONFIDENCE BUILDING for: promote cooperation in regional confidence-building measures (CBMs) INFORMATION EXCHANGE CBM: encourage further analysis and study by research institutes and universities on ICT security related matters
124:1	2016 - U.S.-United Kingdom Cybersecurity Cooperation	2016	urther strengthen and deepen the already extensive cybersecurity cooperation between the United States and the United Kingdom. Both leaders agreed to bolster efforts to enhance the cybersecurity of critical infrastructure in both countries, strengthen threat information sharing and intelligence cooperation on cyber issues, and support new educational exchanges between U.S. and British cybersecurity scholars and researchers.	ASSISTANCE CBM: provide assistance and training to developing countries to improve cybsecurity and ICT use CRITICAL INFRASTRUCTURE for: protecting critical infrastructures EDUCATION for: include cybersecurity courses in school curricula (i.e., primary school, degree courses in undergrad, professional education, and trainings INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information
124:2	2016 - U.S.-United Kingdom Cybersecurity Cooperation	2016	Both governments have agreed to bolster our efforts to increase threat information sharing and conduct joint cybersecurity and network defense exercises to enhance our combined ability to respond to malicious cyber activity	STAKEHOLDER COOPERATION for: conduct joint cybersecurity and/or related law enforcement exercises between nation states
125:1	2016 - United+States-GCC Second+Summit+	2016	GCC countries also supported expanded cooperation on cyber security, endorsing peacetime cyber norms codified by Saudi Arabia, the United States, and other G-20 countries	STATE RESPONSIBILITY for: adhering to rules and regulations agreed upon by previously enacted international law/mandates/treaties
126:1	2016 - India+and+Vietnam+	2016	At the invitation of H. E. Mr. Nguyen Xuan Phuc, Prime Minister of the Socialist Republic of Vietnam, the Prime Minister of the Republic of India H.E. Mr. Narendra Modi paid an Ofcial Visit to the Socialist Republic of Vietnam from 02 - 03 September 2016.	INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information
126:2	2016 - India+and+Vietnam+	2016	The Prime Ministers urged leaders of business and industry to explore new business opportunities in the identifed priority areas for cooperation: hydrocarbons, power generation, renewable energy, infrastructure, tourism, textiles, footwear, medical and pharmaceuticals, ICT, electronics, agriculture, agro- products, chemicals, machine tools and other supporting industries	NORM for: supporting a free and secure internet / cyber space that supports economic growth and innovation
127:1	2016 - Israel+and+U.S.+Cyber+Defense+Cooperation	2016	Israel National Cyber Bureau (INCB) Head Dr. Eviatar Matania and National Cyber Security Authority Head Buky Carmeli have signed a joint declaration on operative cyber defense cooperation between Israel and the US, in the presence of Deputy Secretary of Homeland Security Alejandro Mayorkas and Under Secretary of Homeland Security (National Protection and Programs Directorate) Suzanne Spaulding.	INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information

ID	Document	Document Groups	Quotation Content	Codes
127:2	2016 - Israel+and+U.S.+Cyber+Defense+Cooperation	2016	he cyber defense of critical infrastructures, building partnerships with the private sector and research and development vis-à-vis innovative technologies and solutions.	CRITICAL INFRASTRUCTURE for: protecting critical infrastructures STAKEHOLDER COOPERATION for: encourage participation of other stakeholders such as the private sector, academia, and civil society orgs (as appropriate) for CBM and/or norm creation and implementation STAKEHOLDER COOPERATION for: work with states and/or the private sector/civil society (international and/or domestic) to further cooperate on topics such as law enforcement, prosecution, investment, e-commerce, intellectual property rights, etc.
128:1	2016 - =14th Meeting of Russia, India, & China	2016	The Foreign Ministers of the Russian Federation, the Republic of India and the People's Republic of China held their 14th Meeting in Moscow, Russian Federation, on 18 April 2016.	INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information
128:2	2016 - =14th Meeting of Russia, India, & China	2016	4. The Ministers reiterated their strong commitment to the United Nations as a universal multilateral organization entrusted with the mandate of helping the world community maintain international peace and security, advance common development, promote and protect human rights	HUMAN RIGHTS for: respecting human rights and fundamental freedoms; applying them to cyber space / ICT use, etc. UNITED NATIONS CBM: the United Nations (UN) may serve as an international body for decision-making, framework creation/implementation, and when developing and adopting universally agreed upon ICT norms/rules/principles (in order to ensure peace and responsible behavior/ICT use)
128:3	2016 - =14th Meeting of Russia, India, & China	2016	The Ministers emphasized the need to strengthen cooperation to counter the use of information and communication technologies (ICTs) including the Internet in violation of the UN Charter as well as for terrorist and other criminal purposes. In this regard they reaffirmed common views set forth in the Fortaleza (15 July 2014) and Ufa (9 July 2015) declarations of BRICS summits.	STAKEHOLDER COOPERATION for: work / intensify cooperation against criminal/terrorist use of ICTs STATE RESPONSIBILITY AND SOVEREIGNTY CBM: hold other nation states / entities accountable for actions that may be contrary to the international consensus on responsible State behavior in cyberspace STATE RESPONSIBILITY for: adhering to rules and regulations agreed upon by previously enacted international law/mandates/treaties
128:4	2016 - =14th Meeting of Russia, India, & China	2016	The Ministers reaffirmed the key role of the United Nations in addressing issues of security in the use of ICTs. They support the elaboration and adoption of universal rules of responsible behavior of states in the use of ICTs to prevent conflicts in information space	NORMS CBM: universally agreed upon [voluntary] norms/rules/principles are important for the responsible behavior of States' use of ICTs
128:5	2016 - =14th Meeting of Russia, India, & China	2016	They underlined the importance of providing timely and appropriate responses to requests from one another for information and assistance concerning malicious incidents and activities in the use of ICTs and agreed to cooperate in this area.	CYBER ATTACKS for: responding to requests for help in the event of a cyber attack STATE RESPONSIBILITY for: timely responses to requests for information
128:6	2016 - =14th Meeting of Russia, India, & China	2016	The Ministers advocate a peaceful, open and secure Internet space.	NORM for: promote an open, secure, stable, accessible, and peaceful cyber space / ICT environment
129:1	2015 - 10th IGF Chairs Summary_Finalv2	2015	facilitate increased participation among stakeholders from developing countries and to enhance linkages between the growing number of National and Regional IGF initiatives, the global IGF and the rest of the Internet governance ecosystem	STAKEHOLDER COOPERATION CBM: states should participate and cooperate in multilateral forums
129:2	2015 - 10th IGF Chairs Summary_Finalv2	2015	Creating more awareness about the SDGs, IGF, Multistakeholder mechanisms and how Internet can help achieve SDGs on Regional and National levels, through different stakeholders and Governments.	STAKEHOLDER COOPERATION for: establishing a standing multistakeholder engagement mechanism in order to address stability issues (this includes adequate involvement and consultation of states, non-state actors such as private sector entities, and civil society)
129:3	2015 - 10th IGF Chairs Summary_Finalv2	2015	Inducing more investment into Internet innovation to serve the SDGs, through both public funds and Venture Capital incentives, among other channels.	CONFIDENCE BUILDING CBM: further investments in ICT research and development
129:4	2015 - 10th IGF Chairs Summary_Finalv2	2015	Improving policies serving access, privacy and security of the Internet	ACCESS CBM: access to the internet is an important enabler of development./growth/innovation ACCESS for: support the free flow of information while respecting applicable legal frameworks for privacy and data protection CONFIDENCE BUILDING for: ensuring the free flow of data while also protecting the integrity of that data and the privacy of individual users
129:5	2015 - 10th IGF Chairs Summary_Finalv2	2015	Engaging more Women and youth	DIGITAL EQUALITY for: closing the gender digital divide (focusing on women and girls, but also those a part of gender subgroups such as the LGBTQI+ communiy)
129:6	2015 - 10th IGF Chairs Summary_Finalv2	2015	Extending the Internet economy to marginalized groups and LDCs.	DIGITAL EQUALITY adopted: working towards digital equality and inclusion

ID	Document	Document Groups	Quotation Content	Codes
129:7	2015 - 10th IGF Chairs Summary_Finalv2	2015	Fostering Internet entrepreneurship.	DIGITAL ECONOMY for: fostering safe and secure competition in the digital economy
129:8	2015 - 10th IGF Chairs Summary_Finalv2	2015	Increase knowledge sharing, capacity building and preparation of youth for future employment.	CAPACITY BUILDING CBM: encourage further work in capacity-building EDUCATION CBM: skills development, particularly for younger individuals (both internal and external, international and/or domestic) INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information
129:9	2015 - 10th IGF Chairs Summary_Finalv2	2015	There were calls for further multistakeholder participation in the tackling of cybercrime	STAKEHOLDER COOPERATION for: coordinate/cooperate in combatting cybercrime
129:10	2015 - 10th IGF Chairs Summary_Finalv2	2015	such as the introduction of security elements when developing cyber products and services, was highlighted.	PRODUCT for: developers and producers of products and services should prioritize security and stability
129:11	2015 - 10th IGF Chairs Summary_Finalv2	2015	Participants also stressed the critical role that education plays in addressing cybercrime issues and noted that education should be expanded to involve all levels of society. C	EDUCATION for: implementing [community] education and awareness in order to prevent cybercrime
129:12	2015 - 10th IGF Chairs Summary_Finalv2	2015	There were calls for further multistakeholder participation in the tackling of cybercrime. Session panellists agreed that the IGF, including national and regional IGFs, has proven to be a good collaborative multistakeholder process for cybersecurity, but still needs to reach out to get missing parties around the table. The involvement of the government, private sector, civil society and other stakeholders in handling cyber security was stressed as fundamental in terms of sharing best practices, sharing results of critical assessments and identifying globally accepted standards of cybersecurity	STAKEHOLDER COOPERATION CBM: it is important for other stakeholders such as regional and sub-regional bodies/entities be used to create, promote, and implement CBMs STAKEHOLDER COOPERATION for: encourage participation of other stakeholders such as the private sector, academia, and civil society orgs (as appropriate) for CBM and/or norm creation and implementation STAKEHOLDER COOPERATION for: stakeholders working together on achieving an appropriate balance between the interests of citizens/entities to secure their data, and the needs of law enforcement agencies (while not undermining the fundamentals of technology)
129:13	2015 - 10th IGF Chairs Summary_Finalv2	2015	Discussions about human rights online clearly recognise the particular importance of protecting and promoting privacy, children, minorities, disabled people, and women. • In the future, there is a need to also investigate how cultural diversity can be balanced with access in the context of promoting human rights, and a related demand for supporting indigenous people's needs in terms of cost, access, and needs where cultural and language preservation are concerned. • The need to encourage and promote user trust in technology and education on how to use online platforms in ways that do not infringe others' human rights was stressed. • In the future, it is important that the IGF and other platforms focus on mechanisms for the domestic, regional and international enforcement of human rights and principles; and also refer to and investigate existing legal precedents. The pace of technological change cannot be used as an excuse for inaction, but regulatory responses should be adopted and implemented with caution.	HUMAN RIGHTS CBM: domestic and international cooperation amongst nation states, private sector, civil society, and other non-government entities is important in order to strengthen human rights in cyber space / ICT use, etc. HUMAN RIGHTS for: addressing online gender-abuse/violence through a human rights framework HUMAN RIGHTS for: respecting human rights and fundamental freedoms; applying them to cyber space / ICT use, etc.
129:14	2015 - 10th IGF Chairs Summary_Finalv2	2015	Awareness and literacy programmes are crucial to encourage a better understanding of the problem, along with substantial investment in research and statistics on the incidence of the issue.	EDUCATION for: increased eduation, [digital] literacy, and awareness regarding digital rights and ways to exercise/protect them
131:1	2015 - Joint Statement_ India-Australia Cyber Policy Dialogue	2015	the multi-stakeholder approach to internet governance and cybercrime.	STAKEHOLDER COOPERATION for: coordinate/cooperate in combatting cybercrime STAKEHOLDER COOPERATION for: coordinate/cooperate in preserving multistakeholder internet governance
131:2	2015 - Joint Statement_ India-Australia Cyber Policy Dialogue	2015	the development of international norms of responsible state behaviour in cyberspace, regional developments	NORMS CBM: universally agreed upon [voluntary] norms/rules/principles are important for the responsible behavior of States' use of ICTs
131:3	2015 - Joint Statement_ India-Australia Cyber Policy Dialogue	2015	To strengthen the relationship between CERT-India and CERT-Australia they signed a framework for operational cooperation on cyber security to promote greater cooperation in exchanging information on cyber threats and in responding to incidents.	EMERGENCY RESPONSE CBM: assist in strengthening cooperation amongst national computer ER teams etc. INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information
131:4	2015 - Joint Statement_ India-Australia Cyber Policy Dialogue	2015	cybercrime and on law enforcement measures	STAKEHOLDER COOPERATION for: work with states and/or the private sector/civil society (international and/or domestic) to further cooperate on topics such as law enforcement, prosecution, investment, e-commerce, intellectual property rights, etc.

ID	Document	Document Groups	Quotation Content	Codes
131:5	2015 - Joint Statement_ India-Australia Cyber Policy Dialogue	2015	development of norms including the work of the UN Group of Governmental Expert	UNITED NATIONS for: following the United Nation's (UN) [2015 and or 2013] GGE report's call for all States to be guided in their use of ICTs in relation to the report
131:6	2015 - Joint Statement_ India-Australia Cyber Policy Dialogue	2015	the work of regional bodies including the ASEAN Regional Forum on confdence building and the Asia-Pacifc CERT community in supporting the development of regional CERT capacity	CONFIDENCE BUILDING for: promote cooperation in regional confidence-building measures (CBMs) STAKEHOLDER COOPERATION for: support other international and/or regional cooperative partnerships
132:1	2015 - 1st Australia-Japan Cyber Policy Dialogue	2015	Australia and Japan deepened their understanding of each other's policies and exchanged views on key issues on the international cyber agenda including the development of international norms and the application of international law to state behaviour in cyberspace.	INFORMATION EXCHANGE CBM: exchange national views on the use of ICTS in conflicts INTERNATIONAL LAW CBM: states should publicly express their views on how existing international law applies to activities in cyberspace (in order to improve transparency, etc.) INTERNATIONAL LAW for: applicability of international law to cyberspace
132:2	2015 - 1st Australia-Japan Cyber Policy Dialogue	2015	The inaugural meeting of the Australia-Japan Cyber Policy Dialogue took place in Canberra on Friday 13 February. Prime Minister Tony Abbott and Prime Minister Shinzo Abe agreed on the Dialogue during their summit meeting in Tokyo on 7 April 2014. The Dialogue reflects the two countries' broad and longstanding cooperation on bilateral and global issues	INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information
132:3	2015 - 1st Australia-Japan Cyber Policy Dialogue	2015	also discussed possible bilateral cooperation in areas such as combating cybercrime, critical information infrastructure protection, cybersecurity for major events such as the Tokyo 2020 Olympic and Paralympic Games, and enhancing capacity on cybersecurity among countries of the Asia-Pacific region	CRITICAL INFRASTRUCTURE for: protecting critical infrastructures STAKEHOLDER COOPERATION for: coordinate/cooperate in combatting cybercrime STAKEHOLDER COOPERATION for: support other international and/or regional cooperative partnerships
133:1	2015 - 3rd Japan-US Cyber Dialogue	2015	The 3rd Japan-US Cyber Dialogue will be held in Tokyo on July 22nd, 2015.	INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information
133:2	2015 - 3rd Japan-US Cyber Dialogue	2015	situational awareness, critical infrastructure protection and bilateral cooperation in the international arena.	CRITICAL INFRASTRUCTURE for: protecting critical infrastructures STAKEHOLDER COOPERATION CBM: form bilateral and multilateral cooperation initiatives to build on established partnerships/relationships
134:1	2015 - CSA Signs First International MOU with France	2015	President Tony Tan Keng Yam to the French Republic to mark the 50th anniversary of Singapore-France diplomatic relations. The signing ceremony was witnessed by President Tony Tan and French President Francois Hollande.	INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information
134:2	2015 - CSA Signs First International MOU with France	2015	Mr. David Koh, Chief Executive, CSA said, “This agreement demonstrates the commitment of our organisations to cooperate to face common threats to cyber security. Cyber security is a critical issue in an increasingly borderless world and we look forward to working alongside France to better prevent and respond to evolving cyber threats	STAKEHOLDER COOPERATION CBM: form bilateral and multilateral cooperation initiatives to build on established partnerships/relationships
135:1	2015 - CSA Signs MOU with India	2015	The signing ceremony was held at the Istana and witnessed by Prime Minister Lee Hsien Loong of Singapore, and Prime Minister Narendra Modi of India. Also present at the ceremony was Minister for Communications and Information and Minister-in-Charge of Cyber Security, Dr Yaacob Ibrahim.	INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information
135:2	2015 - CSA Signs MOU with India	2015	CERT- CERT related cooperation for operational readiness and response	EMERGENCY RESPONSE CBM: assist in strengthening cooperation amongst national computer ER teams etc. EMERGENCY RESPONSE CBM: create procedures for mutual assistance in times of incident response
135:3	2015 - CSA Signs MOU with India	2015	exchange of best practices;	INFORMATION EXCHANGE for: sharing of good/best practices in relation to ICTs and cybersecurity
135:4	2015 - CSA Signs MOU with India	2015	professional exchanges of human resource development.	CONFIDENCE BUILDING for: promote human resource development (as related to cyber space, ICTs, cybersecurity, etc.)
136:1	2015 - VII+BRICS+Summit+2015+Ufa+Declaration	2015	We emphasized the importance to strengthen BRICS solidarity and cooperation, and decided to further enhance our strategic partnership on the basis of principles of openness, solidarity, equality and mutual understanding, inclusiveness and mutually beneficial cooperation	INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information STAKEHOLDER COOPERATION CBM: form bilateral and multilateral cooperation initiatives to build on established partnerships/relationships

ID	Document	Document Groups	Quotation Content	Codes
136:2	2015 - VII+BRICS+Summit+2015+Ufa+Declaration	2015	We reaffirmed our strong commitment to the United Nations as a universal multilateral organization entrusted with the mandate of helping the international community maintain international peace and security, advance global development and promote and protect human rights	UNITED NATIONS CBM: the United Nations (UN) may serve as an international body for decision-making, framework creation/implementation, and when developing and adopting universally agreed upon ICT norms/rules/principles (in order to ensure peace and responsible behavior/ICT use)
136:3	2015 - VII+BRICS+Summit+2015+Ufa+Declaration	2015	We expressed our intention to contribute to safeguarding a fair and equitable international order based on the purposes and principles of the UN Charter and to fully avail ourselves of the potential of the Organization as a forum for an open and honest debate as well as coordination of global politics in order to prevent war and conflicts and promote progress and development of humankind	STATE RESPONSIBILITY for: adhering to rules and regulations agreed upon by previously enacted international law/mandates/treaties
136:4	2015 - VII+BRICS+Summit+2015+Ufa+Declaration	2015	sharing of information and best practices relating to security in the use of ICTs	INFORMATION EXCHANGE for: sharing of good/best practices in relation to ICTs and cybersecurity
136:5	2015 - VII+BRICS+Summit+2015+Ufa+Declaration	2015	effective coordination against cyber-crime;	STAKEHOLDER COOPERATION for: coordinate/cooperate in combatting cybercrime
136:6	2015 - VII+BRICS+Summit+2015+Ufa+Declaration	2015	joint research and development projects	CONFIDENCE BUILDING CBM: further investments in ICT research and development INFORMATION EXCHANGE CBM: encourage further analysis and study by research institutes and universities on ICT security related matters INFORMATION EXCHANGE CBM: encouraging exchanges between research and academic institutions
136:7	2015 - VII+BRICS+Summit+2015+Ufa+Declaration	2015	capacity building; and the development of international norms, principles and standards	CAPACITY BUILDING CBM: encourage further work in capacity-building NORMS CBM: further dialogue regarding norms pertaining to State use of ICTs
136:8	2015 - VII+BRICS+Summit+2015+Ufa+Declaration	2015	We support the inclusion of ICT-related issues in the post-2015 development agenda and greater access to ICTs to empower women as well as vulnerable groups to meet the objectives of the agenda	DIGITAL EQUALITY CBM: work towards digital equality and inclusion (i.e., for women and traditionally marginalised groups) - this includes cooperation between the private sector, civil society, and national governments (as well as multilateral banks, and international entities such as the United Nations) DIGITAL EQUALITY for: closing the gender digital divide (focusing on women and girls, but also those a part of gender subgroups such as the LGBTQI+ communiy) DIGITAL EQUALITY for: the protection of digital rights should be embedded in an inclusive approach (i.e., also considers the needs/rights of vulnerable groups such as children, women, gender minorities, people w/ disabilities, etc.)
136:9	2015 - VII+BRICS+Summit+2015+Ufa+Declaration	2015	We also recognize the potential of developing countries in the ICT ecosystem and acknowledge that they have an important role to play in addressing the ICT-related issues in the post-2015 development agenda.	ASSISTANCE CBM: provide assistance and training to developing countries to improve cybsecurity and ICT use
136:10	2015 - VII+BRICS+Summit+2015+Ufa+Declaration	2015	We reiterate the inadmissibility of using ICTs and the Internet to violate human rights and fundamental freedoms, including the right to privacy, and reaffirm that the same rights that people have offline must also be protected online.	ACCESS for: support the free flow of information while respecting applicable legal frameworks for privacy and data protection CONFIDENCE BUILDING for: ensuring the free flow of data while also protecting the integrity of that data and the privacy of individual users HUMAN RIGHTS for: respecting human rights and fundamental freedoms; applying them to cyber space / ICT use, etc.
136:11	2015 - VII+BRICS+Summit+2015+Ufa+Declaration	2015	We agree that the use and development of ICTs through international cooperation and universally accepted norms and principles of international law is of paramount importance in order to ensure a peaceful, secure and open digital and Internet space	INTERNATIONAL LAW for: applicability of international law to cyberspace
136:12	2015 - VII+BRICS+Summit+2015+Ufa+Declaration	2015	as well as violation of the sovereignty of States and of human rights, in particular, the right to privacy	STATE SOVEREIGNTY for: state sovereignty applied to State's ICT activities & ICT infrastructure within their territory

ID	Document	Document Groups	Quotation Content	Codes
136:13	2015 - VII+BRICS+Summit+2015+Ufa +Declaration	2015	We also stress the need to promote cooperation among our countries to combat the use of ICTs for criminal and terrorist purposes.	CYBER ATTACKS for: strengthen tools and resources needed to prepare, deter, defend, and respond to unlawful use of ICTs, cyber attacks / acts of cyber crime and/or terrorism STAKEHOLDER COOPERATION for: coordinate/cooperate in combatting cybercrime
137:1	2015 - U.K.-China+Joint+Statement	2015	At the invitation of Her Majesty Queen Elizabeth II of the United Kingdom of Great Britain and Northern Ireland, His Excellency President Xi Jinping of the People's Republic of China undertook a State Visit to the UK from 19 to 23 October 2015. During the visit, President Xi was received by Her Majesty and senior members of the Royal Family, and held extensive in-depth discussions with Prime Minister David Cameron at No. 10 Downing Street, his Chequers residence, and during a visit to Manchester.	INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information
137:2	2015 - U.K.-China+Joint+Statement	2015	In the last decade, the bilateral relationship has flourished and matured with close high-level exchanges, deeper political trust, fruitful economic cooperation and wider people-to-people contact.	STAKEHOLDER COOPERATION CBM: form bilateral and multilateral cooperation initiatives to build on established partnerships/relationships
137:3	2015 - U.K.-China+Joint+Statement	2015	The UK and China agree to establish a high-level security dialogue to strengthen exchanges and cooperation on security issues such as non-proliferation, organised crime, cyber crime and illegal immigration.	STAKEHOLDER COOPERATION for: coordinate/cooperate in combatting cybercrime
137:4	2015 - U.K.-China+Joint+Statement	2015	The UK and China agree not to conduct or support cyber-enabled theft of intellectual property, trade secrets or confidential business information with the intent of providing competitive advantage	CYBER ATTACK for: preventing ICT-enabled theft of intellectual property (this includes trade secrets and other confidential business information) STATE RESPONSIBILITY & SOVEREIGNTY against: conducting or supporting ICT-enabled theft of intellectual property, trade secrets, or other confidential business info
137:5	2015 - U.K.-China+Joint+Statement	2015	The two sides agree to strengthen cooperation on settling international and regional disputes peacefully in accordance with the UN Charter and international law.	STATE RESPONSIBILITY for: adhering to rules and regulations agreed upon by previously enacted international law/mandates/treaties
139:1	2015 - 2015 - Russia-China+Cybersecurity+Agreement.ru.en	2015	In accordance with paragraph 1 of Article 11 of the Federal Law "On International treaties Russian Federation " approve submitted MFA Of Russia agreed from others interested federal executive authorities and a draft Agreement previously worked out with the Chinese Party between The government Russian Federation and the Government of the People's Republic of China on cooperation in the field of international information security (attached). To instruct the Russian Foreign Ministry to conduct negotiations with the Chinese side and upon reaching an agreement to sign the said Agreement on behalf of the Government of the Russian Federation, authorizing amendments to the attached draft that are not of a fundamental nature.	INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information
139:2	2015 - 2015 - Russia-China+Cybersecurity+Agreement.ru.en	2015	reaffirming that state sovereignty and international norms and principles arising from state sovereignty apply to the behavior of states in the framework of activities related to from using information and communication technologies, and jurisdiction states over information 2 infrastructure on their territory, as well as the fact that the state has the sovereign right to determine and conduct state policy on issues related to the information and telecommunications network "Internet", including ensuring security,	STATE SOVEREIGNTY disagreement: finding States at fault for internationally recognized wrongful ICT acts committed by on state territory STATE SOVEREIGNTY for: state sovereignty applied to State's ICT activities & ICT infrastructure within their territory
139:3	2015 - 2015 - Russia-China+Cybersecurity+Agreement.ru.en	2015	taking into account the important role of information security in ensuring human and civil rights and fundamental freedoms, giving important value balance between providing safety and respect for human rights in the use of information and communication technologies	HUMAN RIGHTS for: respecting human rights and fundamental freedoms; applying them to cyber space / ICT use, etc.
139:4	2015 - 2015 - Russia-China+Cybersecurity+Agreement.ru.en	2015	striving to form a multilateral, democratic and transparent international system of management of the information and telecommunication network "Internet" in order to internationalize the management of the information and telecommunication network "Internet" and ensure equal rights of states to participate in this process, including democratic management of the main resources of the information and telecommunication network "Internet" and their fair distribution,	STAKEHOLDER COOPERATION for: coordinate/cooperate in preserving multistakeholder internet governance
139:5	2015 - 2015 - Russia-China+Cybersecurity+Agreement.ru.en	2015	5) information exchange and cooperation in law enforcement areas for the investigation of cases related to the use of information and communication technologies for terrorist and criminal purposes;	STAKEHOLDER COOPERATION for: stakeholders working together on achieving an appropriate balance between the interests of citizens/entities to secure their data, and the needs of law enforcement agencies (while not undermining the fundamentals of technology)

ID	Document	Document Groups	Quotation Content	Codes
139:6	2015 - 2015 - Russia-China+Cybersecurity+Agreement.ru.en	2015	7) cooperation between the competent authorities of states Parties in areas securing security critical information infrastructure states Parties, exchange technologies and cooperation between the authorized bodies of the states of the Parties in the field of response to computer inciden	CRITICAL INFRASTRUCTURE for: protecting critical infrastructures
139:7	2015 - 2015 - Russia-China+Cybersecurity+Agreement.ru.en	2015	11) deepening cooperation and coordination of activities states Parties by problems securing international information security within the framework of international organizations and forums (including the United Nations	STAKEHOLDER COOPERATION CBM: states should participate and cooperate in multilateral forums UNITED NATIONS CBM: the United Nations (UN) may serve as an international body for decision-making, framework creation/implementation, and when developing and adopting universally agreed upon ICT norms/rules/principles (in order to ensure peace and responsible behavior/ICT use)
139:8	2015 - 2015 - Russia-China+Cybersecurity+Agreement.ru.en	2015	12) promotion of scientific research in the field of providing international information security, joint research work	CONFIDENCE BUILDING CBM: further investments in ICT research and development INFORMATION EXCHANGE CBM: encourage further analysis and study by research institutes and universities on ICT security related matters INFORMATION EXCHANGE CBM: encouraging exchanges between research and academic institutions
139:9	2015 - 2015 - Russia-China+Cybersecurity+Agreement.ru.en	2015	13) joint training of specialists, student exchange, postgraduate students and teachers of specialized higher educational institutions;	EDUCATION CBM: skills development, particularly for younger individuals (both internal and external, international and/or domestic) EDUCATION for: implementing [community] education and awareness in order to prevent cybercrime EDUCATION for: include cybersecurity courses in school curricula (i.e., primary school, degree courses in undergrad, professional education, and trainings EDUCATION for: increased eduation, [digital] literacy, and awareness regarding digital rights and ways to exercise/protect them
139:10	2015 - 2015 - Russia-China+Cybersecurity+Agreement.ru.en	2015	) creating a mechanism for cooperation between authorized authorities of the states of the Parties for the purpose of exchanging information and sharing information on existing and potential risks, threats and vulnerabilities in the field of information security, identifying, assessing, studying, mutual information about them, as well as preventing their occurrence	STAKEHOLDER COOPERATION for: establishing a standing multistakeholder engagement mechanism in order to address stability issues (this includes adequate involvement and consultation of states, non-state actors such as private sector entities, and civil society)
140:1	2015 - President Xi Jinping's State Visit to the United States	2015	timely responses should be provided to requests for information and assistance concerning malicious cyber activities.	STATE RESPONSIBILITY for: timely responses to requests for information
140:2	2015 - President Xi Jinping's State Visit to the United States	2015	Further, both sides agree to cooperate, in a manner consistent with their respective national laws and relevant international obligations, with requests to investigate cybercrimes, collect electronic evidence, and mitigate malicious cyber activity emanating from their territory.	STAKEHOLDER COOPERATION for: coordinate/cooperate in combatting cybercrime STATE RESPONSIBILITY & SOVEREIGNTY for: ensuring that one's territory is not used by non-State actors to commit internationally wrongful acts using ICTs STATE RESPONSIBILITY for: adhering to rules and regulations agreed upon by previously enacted international law/mandates/treaties STATE SOVEREIGNTY for: state sovereignty applied to State's ICT activities & ICT infrastructure within their territory
140:3	2015 - President Xi Jinping's State Visit to the United States	2015	The United States and China agree that neither country's government will conduct or knowingly support cyber-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	CYBER ATTACK for: preventing ICT-enabled theft of intellectual property (this includes trade secrets and other confidential business information) STATE RESPONSIBILITY & SOVEREIGNTY against: conducting or supporting ICT-enabled theft of intellectual property, trade secrets, or other confidential business info

ID	Document	Document Groups	Quotation Content	Codes
140:4	2015 - President Xi Jinping's State Visit to the United States	2015	Both sides are committed to making common effort to further identify and promote appropriate norms of state behavior in cyberspace within the international community. The United States and China welcome the July 2015 report of the UN Group of Governmental Experts in the Field of Information and Telecommunications in the Context of International security, which addresses norms of behavior and other crucial issues for international security in cyberspace. The two sides also agree to create a senior experts group for further discussions on this topic	NORMS CBM: further dialogue regarding norms pertaining to State use of ICTs STAKEHOLDER COOPERATION CBM: form bilateral and multilateral cooperation initiatives to build on established partnerships/relationships STAKEHOLDER COOPERATION CBM: states should participate and cooperate in multilateral forums UNITED NATIONS for: following the United Nation's (UN) [2015 and or 2013] GGE report's call for all States to be guided in their use of ICTs in relation to the report
140:5	2015 - President Xi Jinping's State Visit to the United States	2015	The United States and China agree to establish a high-level joint dialogue mechanism on fighting cybercrime and related issues. China will designate an official at the ministerial level to be the lead and the Ministry of Public Security, Ministry of State Security, Ministry of Justice, and the State Internet and Information Office will participate in the dialogue. The U.S. Secretary of Homeland Security and the U.S. Attorney General will co-chair the dialogue, with participation from representatives from the Federal Bureau of Investigation, the U.S. Intelligence Community and other agencies, for the United States. This mechanism will be used to review the timeliness and quality of responses to requests for information and assistance with respect to malicious cyber activity of concern identified by either side.	STAKEHOLDER COOPERATION CBM: exchange of personnel STAKEHOLDER COOPERATION for: coordinate/cooperate in combatting cybercrime
141:1	2015 - U.S.-E.U.+Cyber+Dialogue	2015	On the occasion of the second meeΘng of the U.S.-EU Cyber Dialogue in Washington, DC on December 7, 2015, the parΘcipants jointly afrmed specifc areas of collaboraΘon and cooperaΘon as follows:	INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information
141:2	2015 - U.S.-E.U.+Cyber+Dialogue	2015	The parΘcipants welcomed the landmark consensus of the 2014-2015 Group of Governmental Experts on Developments in the Field of InformaΘon and TelecommunicaΘons in the Context of InternaΘonal Security, including the afrmaΘon of the applicability of exisΘng internaΘonal law to cyberspace and the arΘculaΘon of norms of responsible state behavior in cyberspac	INTERNATIONAL LAW for: applicability of international law to cyberspace UNITED NATIONS for: following the United Nation's (UN) [2015 and or 2013] GGE report's call for all States to be guided in their use of ICTs in relation to the report
141:3	2015 - U.S.-E.U.+Cyber+Dialogue	2015	Both sides also afrmed the importance of developing confdence building measures within the OrganizaΘon for Security CooperaΘon in Europe, welcomed the conΘnued implementaΘon of the frst set, and urged agreement on further sets of confdence building measures in order to reinforce cooperaΘon, build trust, and reduce the prospects for confict in cyberspace	CONFIDENCE BUILDING CBM: CBM are important for increasing transparency, predictability, and stability CONFIDENCE BUILDING CBM: promote the use of ICTs for peaceful purposes
141:4	2015 - U.S.-E.U.+Cyber+Dialogue	2015	They commended eforts to expand similar acΘviΘes in other regional fora such as the ASEAN Regional Forum and the OrganizaΘon for American States through workshops and other engagements	STAKEHOLDER COOPERATION for: support other international and/or regional cooperative partnerships
141:5	2015 - U.S.-E.U.+Cyber+Dialogue	2015	ll reiterated that no single enΘty, company, organizaΘon or government should seek to control the Internet and expressed their full support for mulΘ-stakeholder governance structures of the Internet that are inclusive, transparent, accountable, and technically sound	CYBERSPACE STABILITY against: any single entity/company/government/inter-governmental organization should seek control of the internet STAKEHOLDER COOPERATION for: coordinate/cooperate in preserving multistakeholder internet governance
141:6	2015 - U.S.-E.U.+Cyber+Dialogue	2015	ybercrime: we afrmed our commitment to promote the ConvenΘon on Cybercrime ("Budapest ConvenΘon") in the fght against cybercrime, including by working together in internaΘonal fora. We welcome the most recent parΘes in 2015: Poland, Sri Lanka, and Canada	CONFIDENCE BUILDING CBM: adopt legislative basis for combatting cybercrime (i.e., the Budapest Convention) STAKEHOLDER COOPERATION for: coordinate/cooperate in combatting cybercrime
141:7	2015 - U.S.-E.U.+Cyber+Dialogue	2015	he United States and the EU reafrmed their strong commitment to the promoΘon and protecΘon of human rights. They emphasized that all individuals have the same human rights online and ofine and that states have an obligaΘon to protect those rights in accordance with internaΘonal law. The single, interconnected, global Internet is a unique shared resource that all people should be able to beneft from, to innovate, learn, organize, and communicate, free from censorship or aΣack. The United States and the EU remain commiΣed to working with all stakeholders to bolster the social, poliΘcal, and economic benefts of an open Internet and to condemning eforts by some governments or other actors to exploit the Internet to repress democraΘc acΘvity and aΣack ciΘzens online. In parΘcular, the rights to freedom of expression and privacy, as set out in the InternaΘonal Covenant on Civil and PoliΘcal Rights, in the digital sphere require the aΣenΘon of all stakeholders	HUMAN RIGHTS CBM: domestic and international cooperation amongst nation states, private sector, civil society, and other non-government entities is important in order to strengthen human rights in cyber space / ICT use, etc. HUMAN RIGHTS for: applicability of international human rights law(s) to cyberspace HUMAN RIGHTS for: respecting human rights and fundamental freedoms; applying them to cyber space / ICT use, etc. NORM for: promote an open, secure, stable, accessible, and peaceful cyber space / ICT environment

ID	Document	Document Groups	Quotation Content	Codes
141:8	2015 - U.S.-E.U.+Cyber+Dialogue	2015	The United States and the EU conϴnue to emphasize the importance of bridging the digital divide towards fostering open socieϴes and enabling economic growth and social development. As founding members of the Global Forum for Cyber Experϴse (GFCE), we remain commiΣed to strengthening our internaϴonal cooperaϴon with mulϴstakeholder communiϴes from all regions of the world to develop innovaϴve soluϴons to today's cyber challenges while maximizing the benefts provided by the Internet and ICTs. We welcomed further coordinaϴon among actors globally, parϴcularly within the GFCE, and agreed to conϴnue exchanging views and good pracϴces, as well as stay coordinated on our respecϴve global cyber capacity building iniϴaϴves. The chairs agreed that they will conϴnue their collaboraϴve eforts and convene the U.S.-EU Cyber Dialogue again in approximately one year's ϴme in Brussels, Belgium	CAPACITY BUILDING CBM: develop regional approaches to capacity-building CAPACITY BUILDING CBM: develop strategies for sustanability in ICT security (capacity-building) CAPACITY BUILDING CBM: encourage further work in capacity-building
142:1	2015 - G20+Leader's+Communiqué+11-16-2015	2015	1. We, the Leaders of the G20, met in Antalya on 15-16 November	INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information
142:2	2015 - G20+Leader's+Communiqué+11-16-2015	2015	We commit ourselves to bridge the digital divide. In the ICT environment, just as elsewhere, states have a special responsibility to promote security, stability, and economic ties with other nations	DIGITAL EQUALITY for: closing the digital divide (i.e., by empowering communities to benefit from digital opportunities) NORM for: promote an open, secure, stable, accessible, and peaceful cyber space / ICT environment
142:3	2015 - G20+Leader's+Communiqué+11-16-2015	2015	n support of that objective, we aćrm that no country should conduct or support ICT-enabled theft of intellectual property, including trade secrets or other conĄdential business information, with the intent of providing competitive advantages to companies or commercial sectors	CYBER ATTACK for: preventing ICT-enabled theft of intellectual property (this includes trade secrets and other confidential business information) STATE RESPONSIBILITY & SOVEREIGNTY against: conducting or supporting ICT-enabled theft of intellectual property, trade secrets, or other confidential business info
142:4	2015 - G20+Leader's+Communiqué+11-16-2015	2015	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	ACCESS for: support the free flow of information while respecting applicable legal frameworks for privacy and data protection CONFIDENCE BUILDING for: ensuring the free flow of data while also protecting the integrity of that data and the privacy of individual users HUMAN RIGHTS for: respecting human rights and fundamental freedoms; applying them to cyber space / ICT use, etc.
142:5	2015 - G20+Leader's+Communiqué+11-16-2015	2015	We also note the key role played by the United Nations in developing norms and in this context we welcome the 2015 report of the UN Group of Governmental Experts in the Field of Information and Telecommunications in the Context of International Security, aćrm that international law, and in particular the UN Charter, is applicable to state conduct in the use of ICTs and commit ourselves to the view that all states should abide by norms of responsible state behaviour in the use of ICTs in accordance with UN resolution A/C.1/70/L.45. We are committed to help ensure an environment in which all actors are able to enjoy the beneĄts of secure use of ICTs.	INTERNATIONAL LAW for: applicability of international law to cyberspace STATE RESPONSIBILITY for: adhering to rules and regulations agreed upon by previously enacted international law/mandates/treaties UNITED NATIONS for: following the United Nation's (UN) [2015 and or 2013] GGE report's call for all States to be guided in their use of ICTs in relation to the report
143:1	2015 - Shanghai+Cooperation+Organization+Draft	2015	Recalling its resolutions on the role of science and technology in the context of international security, in which, inter alia, it recognized that scientific and technological developments could have both civilian and military applications and that progress in science and technology for civilian applications needed to be maintained and encouraged, Recalling also its resolutions 53/70 of 4 December 1998, 54/49 of 1 December 1999, 55/28 of 20 November 2000, 56/19 of 29 November 2001, 57/53 of 22 November 2002, 58/32 of 8 December 2003, 59/61 of 3 December 2004, 60/45 of 8 December 2005, 61/54 of 6 December 2006, 62/17 of 5 December 2007, 63/37 of 2 December 2008, 64/25 of 2 December 2009, 65/41 of 8 December 2010, 66/24 of 2 December 2011, 67/27 of 3 December 2012 and 68/243 of 27 December 2013, on developments in the field of information and telecommunications in the context of international security,	STATE RESPONSIBILITY for: adhering to rules and regulations agreed upon by previously enacted international law/mandates/treaties

ID	Document	Document Groups	Quotation Content	Codes
143:2	2015 - Shanghai+Cooperation+Organization+Draft	2015	Recent years have witnessed considerable progress in the development and application of new information and communication technologies, which potentially could be used for purposes that are inconsistent with the objectives of maintaining international stability and security. An international consensus is now emerging on the need to strengthen international cooperation and formulate relevant international norms, in order to address common challenges in the sphere of information security. To that end, China, Russia, Tajikistan and Uzbekistan jointly submitted an international code of conduct for information security to the General Assembly in 2011 at its sixty-sixth session, which was subsequently co-sponsored by Kyrgyzstan and Kazakhstan. The code of conduct gave rise to extensive international attention and discussion after it was distributed as a document of the General Assembly (A/66/359). Consequently, we revised the code of conduct, taking into full consideration the comments and suggestions from all parties. We now have the honour to enclose herewith the Chinese, Russian and English versions of the revised code of conduct (see annex). With this, we hope to push forward the international debate on international norms on information security, and help forge an early consensus on this issue.	INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information
143:3	2015 - Shanghai+Cooperation+Organization+Draft	2015	Underlining the need for enhanced coordination and cooperation among States in combating the criminal misuse of information technologies and, in that context, stressing the role that can be played by the United Nations and other international and regional organizations,	STAKEHOLDER COOPERATION for: coordinate/cooperate in combatting cybercrime STAKEHOLDER COOPERATION for: support other international and/or regional cooperative partnerships UNITED NATIONS CBM: the United Nations (UN) may serve as an international body for decision-making, framework creation/implementation, and when developing and adopting universally agreed upon ICT norms/rules/principles (in order to ensure peace and responsible behavior/ICT use)
143:4	2015 - Shanghai+Cooperation+Organization+Draft	2015	Highlighting the importance of the security, continuity and stability of the Internet and the need to protect the Internet and other information and communication technology networks from threats and vulnerabilities, and reaffirming the need for a common understanding of the issues of Internet security and for further cooperation at the national and international levels	CONFIDENCE BUILDING for: promote the cybersecurity ecosystem CYBER STABILITY for: maintaining a secure, safe, and trustable ICT environment NORM for: promote an open, secure, stable, accessible, and peaceful cyber space / ICT environment
143:5	2015 - Shanghai+Cooperation+Organization+Draft	2015	Reaffirming that policy authority for Internet-related public issues is the sovereign right of States, which have rights and responsibilities for international Internet-related public policy issues,	STATE RESPONSIBILITY AND SOVEREIGNTY CBM: hold other nation states / entities accountable for actions that may be contrary to the international consensus on responsible State behavior in cyberspace STATE SOVEREIGNTY for: state sovereignty applied to State's ICT activities & ICT infrastructure within their territory
143:6	2015 - Shanghai+Cooperation+Organization+Draft	2015	Bearing in mind the assessments and recommendations contained in the report of the Group of Governmental Experts established in 2012 on the basis of equitable geographical distribution, in fulfilment of resolution 66/24, and which, in accordance with its mandate, considered existing and potential threats in the sphere of information security and possible cooperative measures to address them	UNITED NATIONS for: following the United Nation's (UN) [2015 and or 2013] GGE report's call for all States to be guided in their use of ICTs in relation to the report
143:7	2015 - Shanghai+Cooperation+Organization+Draft	2015	Stressing the need for enhanced efforts to close the digital divide by facilitating the transfer of information technology and capacity-building to developing countries in the areas of cybersecurity best practices and training, pursuant to that General Assembly resolutio	DIGITAL EQUALITY for: closing the digital divide (i.e., by empowering communities to benefit from digital opportunities) INFORMATION EXCHANGE for: sharing of good/best practices in relation to ICTs and cybersecurity NORM for: promote cooperation in training to develop ICT/cybersecurity awareness and skills
143:8	2015 - Shanghai+Cooperation+Organization+Draft	2015	(3) Not to use information and communications technologies and information and communications networks to interfere in the internal affairs of other States or with the aim of undermining their political, economic and social stability;	CYBER ATTACKS against: conducting ICT operations intended to disrupt essential infrastructure of political processes (i.e., election processes) CYBER STABILITY for: protecting political systems DIGITAL ECONOMY for: promote resilience of financial services and institutions against malicious use of ICTs

ID	Document	Document Groups	Quotation Content	Codes
143:9	2015 - Shanghai+Cooperation+Organization+Draft	2015	(4) To cooperate in combating criminal and terrorist activities that use information and communications technologies and information and communications networks, and in curbing the dissemination of information that incites terrorism, separatism or extremism or that inflames hatred on ethnic, racial or religious grounds;	CYBER ATTACKS for: strengthen tools and resources needed to prepare, deter, defend, and respond to unlawful use of ICTs, cyber attacks / acts of cyber crime and/or terrorism STAKEHOLDER COOPERATION for: work / intensify cooperation against criminal/terrorist use of ICTs
143:10	2015 - Shanghai+Cooperation+Organization+Draft	2015	To endeavour to ensure the supply chain security of information and communications technology goods and services, in order to prevent other States from exploiting their dominant position in information and communications technologies, including dominance in resources, critical infrastructures, core technologies, information and communications technology goods and services and information and communications networks to undermine States' right to independent control of information and communications technology goods and services, or to threaten their political, economic and social security	CRITICAL INFRASTRUCTURE for: promoting resilience (as related to ICTs,cybersecurity, and related critical infrastructure CRITICAL INFRASTRUCTURE for: protecting critical infrastructures DIGITAL ECONOMY for: further ensuring the integrity of the ICT supply chain DIGITAL ECONOMY for: states are responsible to notify ICT supply chain/product users when significant vulnerabilities are identified
143:11	2015 - Shanghai+Cooperation+Organization+Draft	2015	All States must play the same role in, and carry equal responsibility for, international governance of the Internet, its security, continuity and stability of operation, and its development in a way which promotes the establishment of multilateral, transparent and democratic international Internet governance mechanisms which ensure an equitable distribution of resources, facilitate access for all and ensure the stable and secure functioning of the Internet;	STAKEHOLDER COOPERATION CBM: form bilateral and multilateral cooperation initiatives to build on established partnerships/relationships STAKEHOLDER COOPERATION CBM: states should participate and cooperate in multilateral forums STAKEHOLDER COOPERATION for: coordinate/cooperate in preserving multistakeholder internet governance
144:1	2015 - U.S.-China+Joint+Statement+on+Economic+Relations	2015	the United States welcomes China playing a more active role in and taking on due responsibility for the international financial architecture, as well as expanded bilateral cooperation to address global economic challenges. To this end	INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information STAKEHOLDER COOPERATION CBM: states should participate and cooperate in multilateral forums
144:2	2015 - U.S.-China+Joint+Statement+on+Economic+Relations	2015	oth countries commit that generally applicable measures to enhance information and communication technology cybersecurity in commercial sectors (ICT cybersecurity regulations) should be consistent with WTO agreements, be narrowly tailored, take into account international norms, be nondiscriminatory, and not impose nationality-based conditions or restrictions, on the purchase, sale, or use of ICT products by commercial enterprises unnecessarily.	STAKEHOLDER COOPERATION CBM: cooperation between states/entities (domestic and/or international) is important for furthering economic relationships/development STATE RESPONSIBILITY for: adhering to rules and regulations agreed upon by previously enacted international law/mandates/treaties
144:3	2015 - U.S.-China+Joint+Statement+on+Economic+Relations	2015	The United States and China affirm the importance of developing and protecting intellectual property, including trade secrets, and commit not to advance generally applicable policies or practices that require the transfer of intellectual property rights or technology as a condition of doing business in their respective markets.	CYBER ATTACK for: preventing ICT-enabled theft of intellectual property (this includes trade secrets and other confidential business information)
144:4	2015 - U.S.-China+Joint+Statement+on+Economic+Relations	2015	Both countries affirm that states should not conduct or knowingly support misappropriation of intellectual property, including trade secrets or other confidential business information with the intent of providing competitive advantages to their companies or commercial sectors. Both countries affirm that states and companies should not by illegal methods make use of technology and commercial advantages to gain commercial benefits.	STATE RESPONSIBILITY & SOVEREIGNTY against: conducting or supporting ICT-enabled theft of intellectual property, trade secrets, or other confidential business info
145:1	2015 - cybersecurity action plan (canada and us)	2015	Public Safety (PS) Canada and the Department of Homeland Security (DHS) are pursuing a coordinated approach to enhance the resiliency of our cyber infrastructure. The Cybersecurity Action Plan (the Action Plan) between PS and DHS seeks to enhance the cybersecurity of our nations through increased integration of PS' and DHS' respective national cybersecurity activities and improved collaboration with the private sector. This Action Plan represents just one of many important efforts between Canada and the United States to deepen our already strong bilateral cybersecurity cooperation.	INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information
145:2	2015 - cybersecurity action plan (canada and us)	2015	The Action Plan's goals and objectives are to be conducted in accordance with the June 2012 Statement of Privacy Principles by the United States and Canada. This Action Plan is intended to remain a living document to be reviewed on a regular basis and updated as needed to support new requirements that align to the Plan's key goals and objectives. It intends to support and inform current and future efforts to advance the goals of Beyond the Border, which ultimately seeks to enhance broad bilateral cooperation on cybersecurity efforts across both governments.	STAKEHOLDER COOPERATION CBM: form bilateral and multilateral cooperation initiatives to build on established partnerships/relationships STATE RESPONSIBILITY for: adhering to rules and regulations agreed upon by previously enacted international law/mandates/treaties
145:3	2015 - cybersecurity action plan (canada and us)	2015	PS' Canadian Cyber Incident Response Centre intends to work jointly with DHS' United States Computer Emergency Readiness Team and Industrial Control Systems Cyber Emergency Response Team towards the following objectives	EMERGENCY RESPONSE CBM: assist in strengthening cooperation amongst national computer ER teams etc. STAKEHOLDER COOPERATION for: conduct joint cybersecurity and/or related law enforcement exercises between nation states

ID	Document	Document Groups	Quotation Content	Codes
145:4	2015 - cybersecurity action plan (canada and us)	2015	Standardize protocols for sharing information.	STATE RESPONSIBILITY for: timely responses to requests for information
147:1	2015 - U.S.-China+High-Level+Joint+Dialogue+on+Cybercrime	2015	On Dec. 1, 2015, in Washington, D.C., Attorney General Loretta E. Lynch and Department of Homeland Security Secretary Jeh Johnson, together with Chinese State Councilor Guo Shengkun, co-chaired the first U.S.-China High- Level Joint Dialogue on Cybercrime and Related Issues.	INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information STAKEHOLDER COOPERATION CBM: form bilateral and multilateral cooperation initiatives to build on established partnerships/relationships
147:2	2015 - U.S.-China+High-Level+Joint+Dialogue+on+Cybercrime	2015	dialogue were to review the timeliness and quality of responses to requests for information and assistance with respect to cybercrime or other malicious cyber activities and to enhance cooperation between the United States and China on cybercrime and related issues.	STAKEHOLDER COOPERATION for: coordinate/cooperate in combatting cybercrime STATE RESPONSIBILITY for: timely responses to requests for information
147:3	2015 - U.S.-China+High-Level+Joint+Dialogue+on+Cybercrime	2015	Both sides decided to conduct a tabletop exercise in the spring of 2016 on agreed- upon cybercrime, malicious cyber activity and network protection scenarios to increase mutual understanding regarding their respective authorities, processes and procedures. During the tabletop exercise, both sides will assess China's proposal for a seminar on combatting terrorist misuse of technology and communications, and will consider the U.S.'s proposal on inviting experts to conduct network protection exchanges.	EMERGENCY RESPONSE CBM: develop guidance on scenario-based exercises at the policy, operational, and technical level between nation states and their Computer Emergency Response Teams (CERTs) and/or Computer Security Incident Response Teams (CSIRTs) STAKEHOLDER COOPERATION for: conduct joint cybersecurity and/or related law enforcement exercises between nation states
147:4	2015 - U.S.-China+High-Level+Joint+Dialogue+on+Cybercrime	2015	Enhance Cooperation on Combatting Cyber-Enabled Crime and Related Issues. Both sides decided to further develop case cooperation on combatting cyber-enabled crimes, including child exploitation, theft of trade secrets, fraud and misuse of technology and communications for terrorist activities, and to enhance exchanges on network protection. Both sides decided to improve cooperation among the relevant agencies, within the framework of the high-level dialogue, on network protection	CYBER ATTACK for: preventing ICT-enabled theft of intellectual property (this includes trade secrets and other confidential business information) STATE RESPONSIBILITY & SOVEREIGNTY against: conducting or supporting ICT-enabled theft of intellectual property, trade secrets, or other confidential business info
148:1	2015 - First+U.S.-India+Strategic+and+Commercial+Dialogue	2015	United States Secretary of State John Kerry and Secretary of Commerce Penny Pritzker welcomed India's External Affairs Minister Sushma Swaraj and Minister of State for Commerce and Industry Nirmala Sitharaman for the first U.S.- India Strategic and Commercial Dialogue held in Washington DC on 22 September 20	INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information
148:2	2015 - First+U.S.-India+Strategic+and+Commercial+Dialogue	2015	Recognizing the centrality of peacekeeping to the UN's efforts for maintenance of international peace and security, the Sides committed to enhance cooperation in peacekeeping capacity building in third countries with a focus on training aspects for UN peacekeepers, especially in identified African countries	ASSIST for: adopting appropriate policies and measures so that developing countries benefit from the advantages of technological progress (and do not suffer from lack of early adoption) ASSISTANCE CBM: provide assistance and training to developing countries to improve cybsecurity and ICT use
148:3	2015 - First+U.S.-India+Strategic+and+Commercial+Dialogue	2015	The Sides announced that the first ministerial meeting of the India-United States-Japan trilateral would convene on the margins of the UN General Assembly in September 2015. They also welcomed Japan's participation in the MALABAR 2015 naval exercise later this year. The U.S. Side affirms its support for India's membership in the Missile Technology Control Regime at its upcoming plenary, the Nuclear Suppliers Group, and in the other global nonproliferation export control regimes	STAKEHOLDER COOPERATION for: support other international and/or regional cooperative partnerships
148:4	2015 - First+U.S.-India+Strategic+and+Commercial+Dialogue	2015	In order to strengthen institutional cooperation between ministries, the Sides announced a new Diplomacy Partnership between the Department of State and the Ministry of External Affairs which will include a new Policy Planning Dialogue and coordination on the training of their diplomats through collaboration between respective Foreign Service Institutes. They expressed satisfaction at the convening of the first meeting of an upgraded UN and Multilateral Dialogue in February 2015, the first meeting of the Space Security Dialogue in March 2015, and the first India-U.S. consultations on Africa in April 2015.	STAKEHOLDER COOPERATION CBM: form bilateral and multilateral cooperation initiatives to build on established partnerships/relationships
148:5	2015 - First+U.S.-India+Strategic+and+Commercial+Dialogue	2015	The U.S. Side reaffirmed its support for a reformed UN Security Council with India as a permanent member. Both sides committed to ensuring that the Security Council continues to play an effective role in maintaining international peace and security as envisioned in the UN Charter. Both sides are committed to continued engagement on Security Council reform in the UN Intergovernmental Negotiations (IGN) on Security Council Reform.	STATE RESPONSIBILITY for: adhering to rules and regulations agreed upon by previously enacted international law/mandates/treaties UNITED NATIONS CBM: the United Nations (UN) may serve as an international body for decision-making, framework creation/implementation, and when developing and adopting universally agreed upon ICT norms/rules/principles (in order to ensure peace and responsible behavior/ICT use)

ID	Document	Document Groups	Quotation Content	Codes
148:6	2015 - First+U.S.-India+Strategic+and+Commercial+Dialogue	2015	On cyber issues, the Sides supported an open, inclusive, transparent, and multi-stakeholder system of internet governance and planned to work together to promote cyber security, combat cyber crime, and advance norms of responsible state behavior in cyberspace	NORM for: promote an open, secure, stable, accessible, and peaceful cyber space / ICT environment NORMS CBM: further dialogue regarding norms pertaining to State use of ICTs STAKEHOLDER COOPERATION for: coordinate/cooperate in combatting cybercrime
149:1	2015 - U.S.-Japan+Joint+Vision+Statement+4-28-2015	2015	cyber space based on the free flow of information and an open internet;	ACCESS for: support the free flow of information while respecting applicable legal frameworks for privacy and data protection CONFIDENCE BUILDING for: ensuring the free flow of data while also protecting the integrity of that data and the privacy of individual users NORM for: promote an open, secure, stable, accessible, and peaceful cyber space / ICT environment
149:2	2015 - U.S.-Japan+Joint+Vision+Statement+4-28-2015	2015	Today the United States and Japan honor a partnership that for seven decades has made enduring contributions to global peace, security, and prosperity. In this year which marks 70 years since the end of World War II, the relationship between our two countries stands as a SHARE THIS: □ □ □ This is historical material “frozen in time”. The website is no longer updated and links to external websites and some internal pages may not work. □ 3/2/2018 U.S.-Japan Joint Vision Statement | whitehouse.gov https://obamawhitehouse.archives.gov/the-press-office/2015/04/28/us-japan-joint-vision-statement 2/4 model of the power of reconciliation: former adversaries who have become steadfast allies and who work together to advance common interests and universal values in Asia and globally. Together we have helped to build a strong rules-based international order, based on a commitment to rules, norms and institutions that are the foundation of global affairs and our way of life.	INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information
149:3	2015 - U.S.-Japan+Joint+Vision+Statement+4-28-2015	2015	to advance human rights and universal freedoms	DIGITAL EQUALITY CBM: work towards digital equality and inclusion (i.e., for women and traditionally marginalised groups) - this includes cooperation between the private sector, civil society, and national governments (as well as multilateral banks, and international entities such as the United Nations) DIGITAL EQUALITY for: closing the gender digital divide (focusing on women and girls, but also those a part of gender subgroups such as the LGBTQI+ communiy) HUMAN RIGHTS for: respecting human rights and fundamental freedoms; applying them to cyber space / ICT use, etc.
149:4	2015 - U.S.-Japan+Joint+Vision+Statement+4-28-2015	2015	The United States looks forward to a reformed U.N. Security Council that includes Japan as a permanent member. Seventy years ago this partnership was unimaginable. Today it is a fitting reflection of our shared interests, capabilities and values.	UNITED NATIONS CBM: the United Nations (UN) may serve as an international body for decision-making, framework creation/implementation, and when developing and adopting universally agreed upon ICT norms/rules/principles (in order to ensure peace and responsible behavior/ICT use)
149:5	2015 - U.S.-Japan+Joint+Vision+Statement+4-28-2015	2015	based upon international law;	INTERNATIONAL LAW for: applicability of international law to cyberspace
149:6	2015 - U.S.-Japan+Joint+Vision+Statement+4-28-2015	2015	Respect for sovereignty and territorial integrity;	STATE SOVEREIGNTY for: state sovereignty applied to State's ICT activities & ICT infrastructure within their territory
149:7	2015 - U.S.-Japan+Joint+Vision+Statement+4-28-2015	2015	Support for trilateral and multilateral cooperation among like-minded partners.	STAKEHOLDER COOPERATION CBM: form bilateral and multilateral cooperation initiatives to build on established partnerships/relationships STAKEHOLDER COOPERATION CBM: states should participate and cooperate in multilateral forums
150:1	2015 - U.S.-GCC+Camp+David+Joint+Statement	2015	President Obama and Heads of Delegations of the Gulf Cooperation Council (GCC) member states, the Secretary General of the GCC, and members the President’s Cabinet met today at Camp David to reaffirm and deepen the strong partnership and cooperation between the United States and the GCC. The leaders underscored their mutual commitment to a U.S.- GCC strategic partnership to build closer relations in all fields, including defense and security cooperation, and develop collective approaches to regional issues in order to advance their shared interest in stability and prosperity	INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information

ID	Document	Document Groups	Quotation Content	Codes
151:1	2015 - Remarks+by+H.E.+Xi+Jinping+ At+Opening+Ceremony+of+the +2nd+World+Internet+Confere nce	2015	o the second World Internet Conferenc	INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information
151:2	2015 - Remarks+by+H.E.+Xi+Jinping+ At+Opening+Ceremony+of+the +2nd+World+Internet+Confere nce	2015	In the face of these problems and challenges, the international community must enhance dialogue and cooperation on the basis of mutual respect and trust, promote transformation of the global Internet governance system, and work together to foster a peaceful, secure, open and cooperative cyberspace and put in place a multilateral, democratic and transparent global Internet governance system.	STAKEHOLDER COOPERATION CBM: states should participate and cooperate in multilateral forums
151:3	2015 - Remarks+by+H.E.+Xi+Jinping+ At+Opening+Ceremony+of+the +2nd+World+Internet+Confere nce	2015	Respect for cyber sovereignty.	INTERNATIONAL LAW for: applicability of international law to cyberspace STATE SOVEREIGNTY for: state sovereignty applied to State's ICT activities & ICT infrastructure within their territory
151:4	2015 - Remarks+by+H.E.+Xi+Jinping+ At+Opening+Ceremony+of+the +2nd+World+Internet+Confere nce	2015	- Maintenance of peace and securit	CONFIDENCE BUILDING for: promote the cybersecurity ecosystem NORM for: promote an open, secure, stable, accessible, and peaceful cyber space / ICT environment STATE RESPONSIBILITY for: states should behave responsibly in cyberspace (and use ICTs responsibly) during peacetime
151:5	2015 - Remarks+by+H.E.+Xi+Jinping+ At+Opening+Ceremony+of+the +2nd+World+Internet+Confere nce	2015	All cyber crimes, be they commercial cyber thefts or hacker attacks against government networks, should be firmly combated in accordance with relevant laws and international conventions	CONFIDENCE BUILDING CBM: adopt legislative basis for combatting cybercrime (i.e., the Budapest Convention) STATE RESPONSIBILITY for: adhering to rules and regulations agreed upon by previously enacted international law/mandates/treaties STATE RESPONSIBILITY for: states must meet international obligations regarding internationally wrongful acts attributed to them
151:6	2015 - Remarks+by+H.E.+Xi+Jinping+ At+Opening+Ceremony+of+the +2nd+World+Internet+Confere nce	2015	First, speed up the building of global Internet infrastructure and promote inter-connectivity.	ACCESS CBM: access to the internet is an important enabler of development./growth/innovation ACCESS CBM: creating a free flow of and acccess to the internet is essential for the digital economy, and beneficial to development ACCESS for: support the free flow of information while respecting applicable legal frameworks for privacy and data protection
151:7	2015 - Remarks+by+H.E.+Xi+Jinping+ At+Opening+Ceremony+of+the +2nd+World+Internet+Confere nce	2015	Third, promote innovative development of cyber economy for common prosperity	CONFIDENCE BUILDING CBM: recognize importance of ICTs as the key driver of governance, economy, commerce, trade, and social well-being DIGITAL ECONOMY disagreement: updating international trade rules and procedures to better cater for the digital era DIGITAL ECONOMY for: fostering safe and secure competition in the digital economy
151:8	2015 - Remarks+by+H.E.+Xi+Jinping+ At+Opening+Ceremony+of+the +2nd+World+Internet+Confere nce	2015	Fifth, build an Internet governance system to promote equity and justice	STAKEHOLDER COOPERATION for: coordinate/cooperate in preserving multistakeholder internet governance
152:1	2015 - Joint+Statement+President+Ob ama+and+Prime+Minister+Shar if+(Pakistan)	2015	At the invitation of President Obama, Prime Minister Sharif paid an official visit to Washington from October 20 to 23, 2015 that reinforced the commitment of both leaders to an enduring U.S.-Pakistan partnership, a prosperous Pakistan, and a more stable region. President Obama and Prime Minister Sharif held wide-ranging discussions at the White House today. The two leaders expressed their conviction that a resilient U.S.-Pakistan partnership is vital to regional and global peace and security and reaffirmed their commitment to address evolving threats in South Asia.	INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information

ID	Document	Document Groups	Quotation Content	Codes
152:2	2015 - Joint+Statement+President+Obama+and+Prime+Minister+Sharif+(Pakistan)	2015	consensus report of the 2015 UN Group of Governmental Experts in the Field of Information and Telecommunications in the Context of International Security. The leaders looked forward to further multilateral engagement, and discussion of cyber issues as part of the U.S.- Pakistan Strategic Dialogue	STAKEHOLDER COOPERATION CBM: form bilateral and multilateral cooperation initiatives to build on established partnerships/relationships STAKEHOLDER COOPERATION CBM: states should participate and cooperate in multilateral forums UNITED NATIONS for: following the United Nation's (UN) [2015 and or 2013] GGE report's call for all States to be guided in their use of ICTs in relation to the report
153:1	2015 - Remarks+by+Secretary+Carter+and+Minister+Han (US and South Korea)	2015	It's been my privilege to host Korean Minister of National Defense Han Min Koo here for what is the 48th U.S.-Republic of Korea security consultative meeting. These meetings are valuable opportunities for our nations to come together to address shared security challenges.	INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information
153:2	2015 - Remarks+by+Secretary+Carter+and+Minister+Han (US and South Korea)	2015	The DOD and the MND have agreed to further strengthen defense cyber cooperation to effectively respond to North Korea cyber attacks and threats. To this end, we will operate a bilateral cyber working group task force from October to reach specific measures for bilateral cyber cooperation.	CONFIDENCE BUILDING for: promote cooperation in regional confidence-building measures (CBMs) INFORMATION EXCHANGE for: increasing international cooperation is required to address cyber security risks STAKEHOLDER COOPERATION CBM: form bilateral and multilateral cooperation initiatives to build on established partnerships/relationships
154:1	2015 - US - South Korea	2015	First, no country should conduct or knowingly support online activity that intentionally damages or impedes the use of another country's critical infrastructure	CRITICAL INFRASTRUCTURE against: knowingly damaging critical infrastructure CRITICAL INFRASTRUCTURE against: knowingly support cyberactivity that intentionally damages or impairs the use and operation of critical infrastructure CRITICAL INFRASTRUCTURE for: promoting resilience (as related to ICTs,cybersecurity, and related critical infrastructure CRITICAL INFRASTRUCTURE for: protecting critical infrastructures
154:2	2015 - US - South Korea	2015	Second, no country should seek either to prevent emergency teams from responding to a cybersecurity incident, or allow its own teams to cause harm	CYBER ATTACKS against: states using authorized emergency response teams to engage in malicuous / harmful international activity CYBER ATTACKS against: targeting emergency response teams
154:3	2015 - US - South Korea	2015	Third, no country should conduct or support cyber-enabled theft of / intellectual property, trade secrets, or other confidential business information for commercial gain	CYBER ATTACK for: preventing ICT-enabled theft of intellectual property (this includes trade secrets and other confidential business information) STATE RESPONSIBILITY & SOVEREIGNTY against: conducting or supporting ICT-enabled theft of intellectual property, trade secrets, or other confidential business info
154:4	2015 - US - South Korea	2015	Fourth, every country should mitigate malicious cyber activity emanating from its soil, and they should do so in a transparent, accountable and cooperative way. And fifth, every country should do what it can to help states that are victimized by a cyberattack.	CYBER ATTACKS against: states knowingly allowing their territory to be used for internationally wrongful acts using ICTs STATE RESPONSIBILITY & SOVEREIGNTY for: ensuring that one's territory is not used by non-State actors to commit internationally wrongful acts using ICTs STATE SOVEREIGNTY for: state sovereignty applied to State's ICT activities & ICT infrastructure within their territory
154:5	2015 - US - South Korea	2015	To build trust, the UN Group of Governmental Experts has stressed the importance of high-level communication, transparency about national policies, dispute settlement mechanisms, and the timely sharing of information – all of them, very sound and important thoughts.	UNITED NATIONS for: following the United Nation's (UN) [2015 and or 2013] GGE report's call for all States to be guided in their use of ICTs in relation to the report
154:6	2015 - US - South Korea	2015	And that's precisely why the United States is working with partners on every continent to strengthen the capacity of governments to prevent cyber-crime through improved training, the right legal frameworks, information sharing, and public involvement.	STAKEHOLDER COOPERATION for: coordinate/cooperate in combatting cybercrime
154:7	2015 - US - South Korea	2015	I introduced legislation to protect the privacy rights of individuals and I still feel very strongly about that principle. And we are working to make sure we protect the privacy of people, not just in our country but in othe	DIGITAL EQUALITY for: the protection of digital rights should be embedded in an inclusive approach (i.e., also considers the needs/rights of vulnerable groups such as children, women, gender minorities, people w/ disabilities, etc.) HUMAN RIGHTS for: respecting human rights and fundamental freedoms; applying them to cyber space / ICT use, etc.

ID	Document	Document Groups	Quotation Content	Codes
154:8	2015 - US - South Korea	2015	The best vehicle for international cooperation in this field is the Budapest Convention on Cybercrime, which my government urges every nation to consider joining. There is no better legal framework for working across borders to define what cybercrime is and how breaches of the law should be prevented and prosecuted. We also support the G-7 24/7 Network – in which South Korea is an active participant – and that enables police and prosecutors from more than 70 countries to request rapid assistance on their investigations.	CONFIDENCE BUILDING CBM: adopt legislative basis for combatting cybercrime (i.e., the Budapest Convention) STATE RESPONSIBILITY for: adhering to rules and regulations agreed upon by previously enacted international law/mandates/treaties
155:1	2015 - Fact Sheet_ The United States-Republic of Korea Alliance_	2015	The United States and the ROK remain committed to expanded cooperation on cyber issues with a view to ensuring the continued openness and enhanced security of cyberspace. We affirm that cyberspace should remain a driving force for freedom, prosperity, and economic growth, and noted a shared commitment to the multi-stakeholder model of Internet governance, and for ensuring the free flow of information	ACCESS CBM: creating a free flow of and acccess to the internet is essential for the digital economy, and beneficial to development ACCESS for: support the free flow of information while respecting applicable legal frameworks for privacy and data protection CONFIDENCE BUILDING for: ensuring the free flow of data while also protecting the integrity of that data and the privacy of individual users INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information STAKEHOLDER COOPERATION CBM: form bilateral and multilateral cooperation initiatives to build on established partnerships/relationships STAKEHOLDER COOPERATION CBM: states should participate and cooperate in multilateral forums STAKEHOLDER COOPERATION for: coordinate/cooperate in preserving multistakeholder internet governance
155:2	2015 - Fact Sheet_ The United States-Republic of Korea Alliance_	2015	The United States and the ROK share the view that in cyberspace, just as elsewhere, states have a special responsibility to promote security, stability, and economic ties with other nations. In support of that objective, we formally endorse the 2015 report of the UN Group of Governmental Experts in the Field of Information and Telecommunications in the Context of International Security.	NORM for: promote an open, secure, stable, accessible, and peaceful cyber space / ICT environment UNITED NATIONS for: following the United Nation's (UN) [2015 and or 2013] GGE report's call for all States to be guided in their use of ICTs in relation to the report
155:3	2015 - Fact Sheet_ The United States-Republic of Korea Alliance_	2015	Both governments further affirm that international law is applicable to state conduct in cyberspace and that additional, voluntary norms of state behavior in cyberspace during peacetime also could contribute to international stability. I	INTERNATIONAL LAW for: applicability of international law to cyberspace
155:4	2015 - Fact Sheet_ The United States-Republic of Korea Alliance_	2015	no country should conduct or knowingly support online activity that intentionally damages critical infrastructure or impairs the use of it to provide services to the public	CRITICAL INFRASTRUCTURE against: knowingly damaging critical infrastructure CRITICAL INFRASTRUCTURE against: knowingly support cyberactivity that intentionally damages or impairs the use and operation of critical infrastructure CRITICAL INFRASTRUCTURE for: promoting resilience (as related to ICTs,cybersecurity, and related critical infrastructure CRITICAL INFRASTRUCTURE for: protecting critical infrastructures
155:5	2015 - Fact Sheet_ The United States-Republic of Korea Alliance_	2015	o country should conduct or knowingly support cyber-enabled theft of intellectual property, trade secrets, or other confidential business information with the intent of providing competitive advantages to its companies or commercial sectors;	CYBER ATTACK for: preventing ICT-enabled theft of intellectual property (this includes trade secrets and other confidential business information) STATE RESPONSIBILITY & SOVEREIGNTY against: conducting or supporting ICT-enabled theft of intellectual property, trade secrets, or other confidential business info
155:6	2015 - Fact Sheet_ The United States-Republic of Korea Alliance_	2015	every country should cooperate, consistent with its domestic 11/24/2020 Joint Fact Sheet: The United States-Republic of Korea Alliance: Shared Values, New Frontiers | whitehouse.gov https://obamawhitehouse.archives.gov/the-press-office/2015/10/16/joint-fact-sheet-united-states-republic-korea-alliance-shared-values-new 9/11 law and international obligations, with requests for assistance from other states in investigating cybercrime or the use of information and communication technologies for terrorist purposes or to mitigate such activity emanating from its territory	CYBER ATTACKS against: states knowingly allowing their territory to be used for internationally wrongful acts using ICTs CYBER ATTACKS for: responding to requests for help in the event of a cyber attack DOMESTIC LAW for: applicability of domestic law to cyber space / ICT usage STATE RESPONSIBILITY & SOVEREIGNTY for: ensuring that one's territory is not used by non-State actors to commit internationally wrongful acts using ICTs STATE RESPONSIBILITY for: timely responses to requests for information STATE SOVEREIGNTY for: state sovereignty applied to State's ICT activities & ICT infrastructure within their territory

ID	Document	Document Groups	Quotation Content	Codes
155:7	2015 - Fact Sheet_ The United States-Republic of Korea Alliance_	2015	or these voluntary norms is crucial to increasing transparency and stability among all nations in cyberspace.	NORMS CBM: universally agreed upon [voluntary] norms/rules/principles are important for the responsible behavior of States' use of ICTs
155:8	2015 - Fact Sheet_ The United States-Republic of Korea Alliance_	2015	(1) enhancing information sharing on cyber threats, particularly to critical infrastructure	INFORMATION EXCHANGE for: furthering future dialogue/cooperation for a safe, open, and secure internet/cyberspace
155:9	2015 - Fact Sheet_ The United States-Republic of Korea Alliance_	2015	deepening military-to-military cyber cooperation	STATE RESPONSIBILITY for: furthering military to military cyber cooperation
155:10	2015 - Fact Sheet_ The United States-Republic of Korea Alliance_	2015	Our affirmation of the applicability of international law and support for these voluntary norms is crucial to increasing transparency and stability among all nations in cyberspace	CONFIDENCE BUILDING CBM: voluntary transparency INTERNATIONAL LAW for: applicability of international law to cyberspace
155:11	2015 - Fact Sheet_ The United States-Republic of Korea Alliance_	2015	In addition, The United States and the ROK decided to establish a White House – Blue House cyber coordination channel to further strengthen and complement the deep and broad bilateral cyber cooperation that already exists between our two countries.	STAKEHOLDER COOPERATION CBM: form bilateral and multilateral cooperation initiatives to build on established partnerships/relationships STAKEHOLDER COOPERATION CBM: states should participate and cooperate in multilateral forums
156:1	2015 - EU+Council+Conclusions+on+ Cyber+Diplomacy	2015	supporting the efforts of third countries to increase and improve their citizens' access to and secure use of information and communication technology (ICT) and the Internet,	ASSIST for: adopting appropriate policies and measures so that developing countries benefit from the advantages of technological progress (and do not suffer from lack of early adoption) ASSISTANCE CBM: provide assistance and training to developing countries to improve cybsecurity and ICT use
156:2	2015 - EU+Council+Conclusions+on+ Cyber+Diplomacy	2015	raising awareness and empowering stakeholders to use ICT and the Internet to promote human rights and fundamental freedoms in cyberspace	HUMAN RIGHTS for: respecting human rights and fundamental freedoms; applying them to cyber space / ICT use, etc. NORM for: promote cooperation in training to develop ICT/cybersecurity awareness and skills
156:3	2015 - EU+Council+Conclusions+on+ Cyber+Diplomacy	2015	o place specific emphasis on further promoting the EU digital single market and enhancing IT security, promoting digital trust and enabling greater use of ICTs and ICT driven growth	NORM for: promote an open, secure, stable, accessible, and peaceful cyber space / ICT environment NORM for: supporting a free and secure internet / cyber space that supports economic growth and innovation
156:4	2015 - EU+Council+Conclusions+on+ Cyber+Diplomacy	2015	the application of existing international l	INTERNATIONAL LAW for: applicability of international law to cyberspace
156:5	2015 - EU+Council+Conclusions+on+ Cyber+Diplomacy	2015	AFFIRMING that the EU and its Member States should address these cross-cutting multifaceted issues with a coherent international cyberspace policy that promotes EU political, economic and strategic interests and continue to engage with key international partners and organisations as well as with civil society and the private sector	INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information STAKEHOLDER COOPERATION CBM: states should participate and cooperate in multilateral forums STAKEHOLDER COOPERATION for: support other international and/or regional cooperative partnerships
156:6	2015 - EU+Council+Conclusions+on+ Cyber+Diplomacy	2015	REAFFIRMING the EU's position that the same norms, principles and values that the EU upholds offline, notably the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, the European Convention for the Protection of Human Rights and Fundamental Freedoms, the Convention on the Rights of the Child and the EU Charter of Fundamental Rights, should also apply and receive protection in cyberspace,	STATE RESPONSIBILITY for: adhering to rules and regulations agreed upon by previously enacted international law/mandates/treaties
156:7	2015 - EU+Council+Conclusions+on+ Cyber+Diplomacy	2015	access to information and right to privacy,	ACCESS CBM: access to the internet is an important enabler of development./growth/innovation ACCESS CBM: creating a free flow of and acccess to the internet is essential for the digital economy, and beneficial to development ACCESS for: support the free flow of information while respecting applicable legal frameworks for privacy and data protection

ID	Document	Document Groups	Quotation Content	Codes
156:8	2015 - EU+Council+Conclusions+on+ Cyber+Diplomacy	2015	promotes a cyber policy informed by gender equality,	DIGITAL EQUALITY for: closing the gender digital divide (focusing on women and girls, but also those a part of gender subgroups such as the LGBTQI+ communiy) DIGITAL EQUALITY for: engaging policymakers in honest conversations involving gender-related issues in cyberspace DIGITAL EQUALITY for: the protection of digital rights should be embedded in an inclusive approach (i.e., also considers the needs/rights of vulnerable groups such as children, women, gender minorities, people w/ disabilities, etc.)
156:9	2015 - EU+Council+Conclusions+on+ Cyber+Diplomacy	2015	romotes the efforts to strengthen the multi-stakeholder model of Internet governance,	STAKEHOLDER COOPERATION for: coordinate/cooperate in preserving multistakeholder internet governance
156:10	2015 - EU+Council+Conclusions+on+ Cyber+Diplomacy	2015	by strengthening cybersecurity and improving cooperation in fighting cybercrime,	CRITICAL INFRASTRUCTURE for: promoting resilience (as related to ICTs,cybersecurity, and related critical infrastructure STAKEHOLDER COOPERATION for: coordinate/cooperate in combatting cybercrime
156:11	2015 - EU+Council+Conclusions+on+ Cyber+Diplomacy	2015	WELCOMES the work done within the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, notably its 2013 report6, and the consensus achieved that international law, in particular the Charter of the United Nations, is applicable to cyberspace and is essential to reduce risks and maintain peace and stability,	UNITED NATIONS CBM: the United Nations (UN) may serve as an international body for decision-making, framework creation/implementation, and when developing and adopting universally agreed upon ICT norms/rules/principles (in order to ensure peace and responsible behavior/ICT use) UNITED NATIONS for: following the United Nation's (UN) [2015 and or 2013] GGE report's call for all States to be guided in their use of ICTs in relation to the report
156:12	2015 - EU+Council+Conclusions+on+ Cyber+Diplomacy	2015	development of norms for responsible state behaviour in cyberspace with a view to increasing transparency and trust, consistent with existing international law provisions	NORMS CBM: universally agreed upon [voluntary] norms/rules/principles are important for the responsible behavior of States' use of ICTs
156:13	2015 - EU+Council+Conclusions+on+ Cyber+Diplomacy	2015	to strongly uphold the principles regarding State responsibility for internationally wrongful acts and to take the initiatives necessary at national, regional and international level to ensure that they are fully respected and enforced in cyberspace,	STATE RESPONSIBILITY for: states must meet international obligations regarding internationally wrongful acts attributed to them
156:14	2015 - EU+Council+Conclusions+on+ Cyber+Diplomacy	2015	develop a coherent and global approach to cyber capacity building, which on one side brings together technology, policy and skills development within a broader and overreaching EU development and security agenda, and on other side facilitates the design of an effective EU model for cyber capacity building;	CAPACITY BUILDING CBM: assign appropriate weight to ICT security awareness and capacity building in development and assistance planning CAPACITY BUILDING CBM: develop regional approaches to capacity-building CAPACITY BUILDING CBM: develop strategies for sustanability in ICT security (capacity-building) CAPACITY BUILDING CBM: encourage further work in capacity-building
156:15	2015 - EU+Council+Conclusions+on+ Cyber+Diplomacy	2015	make cyber capacity building an integral part of wider global approaches in all cyberspace domains, including through close cooperation with academia and the private sector as well as European Union Network and Information Security Agency (ENISA), the European Cybercrime Centre within Europol and the EU Institute for Security Studies9	STAKEHOLDER COOPERATION for: encourage participation of other stakeholders such as the private sector, academia, and civil society orgs (as appropriate) for CBM and/or norm creation and implementation STAKEHOLDER COOPERATION for: recognizing the private sector's responsibilities in working towards improving trust, security, and stability in cyberspace
156:16	2015 - EU+Council+Conclusions+on+ Cyber+Diplomacy	2015	promote sustainable cyber capacity building, when appropriate, together with international partners, as well as streamlining and prioritising funding, including by making full use of the relevant EU external financial instruments and programmes;	CAPACITY BUILDING CBM: pioritize ICT security awareness and capacity-building in national plans and budgets
156:17	2015 - EU+Council+Conclusions+on+ Cyber+Diplomacy	2015	tackle growing cyber threats and challenges by increasing resilience of critical information infrastructure and by reinforcing close cooperation and coordination among international stakeholders through initiatives such as the development of confidence building, common standards, international cyber exercises, awareness-raising, training, research and education, incident response mechanism	EDUCATION CBM: skills development, particularly for younger individuals (both internal and external, international and/or domestic) EDUCATION for: increased eduation, [digital] literacy, and awareness regarding digital rights and ways to exercise/protect them NORM for: promote cooperation in training to develop ICT/cybersecurity awareness and skills

ID	Document	Document Groups	Quotation Content	Codes
157:1	2014 - 6th+BRICS+Summit+Fortaleza +Declaration	2014	1. We, the leaders of the Federative Republic of Brazil, the Russian Federation, the Republic of India, the People's Republic of China and the Republic of South Africa, met in Fortaleza, Brazil, on 15 July 2014 at the Sixth BRICS Summit. To inaugurate the second cycle of BRICS Summits, the theme chosen for our discussions was "Inclusive Growth: Sustainable Solutions", in keeping with the inclusive macroeconomic and social policies carried out by our governments and the imperative to address challenges to humankind posed by the need to simultaneously achieve growth, inclusiveness, protection and preservation	INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information
157:2	2014 - 6th+BRICS+Summit+Fortaleza +Declaration	2014	We will explore cooperation on combating cybercrimes	STAKEHOLDER COOPERATION for: coordinate/cooperate in combatting cybercrime
157:3	2014 - 6th+BRICS+Summit+Fortaleza +Declaration	2014	We consider that the UN has a central role in this matter. We agree it is necessary to preserve ICTs, particularly the Internet, as an instrument of peace and development and to prevent its use as a weapon.	NORM for: promote an open, secure, stable, accessible, and peaceful cyber space / ICT environment UNITED NATIONS CBM: the United Nations (UN) may serve as an international body for decision-making, framework creation/implementation, and when developing and adopting universally agreed upon ICT norms/rules/principles (in order to ensure peace and responsible behavior/ICT use)
157:4	2014 - 6th+BRICS+Summit+Fortaleza +Declaration	2014	We reiterate the common approach set forth in the eThekwini Declaration about the importance of security in the use of ICTs	STATE RESPONSIBILITY for: adhering to rules and regulations agreed upon by previously enacted international law/mandates/treaties
157:5	2014 - 6th+BRICS+Summit+Fortaleza +Declaration	2014	We call upon all entities to refrain from financing, encouraging, providing training for or otherwise supporting terrorist activities	CYBER ATTACKS for: strengthen tools and resources needed to prepare, deter, defend, and respond to unlawful use of ICTs, cyber attacks / acts of cyber crime and/or terrorism STAKEHOLDER COOPERATION for: work / intensify cooperation against criminal/terrorist use of ICTs
157:6	2014 - 6th+BRICS+Summit+Fortaleza +Declaration	2014	ccordance with international law	INTERNATIONAL LAW for: applicability of international law to cyberspace
157:7	2014 - 6th+BRICS+Summit+Fortaleza +Declaration	2014	with respect to human rights and fundamental freedoms	HUMAN RIGHTS for: respecting human rights and fundamental freedoms; applying them to cyber space / ICT use, etc.
157:8	2014 - 6th+BRICS+Summit+Fortaleza +Declaration	2014	We believe that ICTs should provide instruments to foster sustainable economic progress and social inclusion, working together with the ICT industry, civil society and academia in order to realize the ICT-related potential opportunities and benefits for al	ACCESS CBM: creating a free flow of and acccess to the internet is essential for the digital economy, and beneficial to development CONFIDENCE BUILDING CBM: recognize importance of ICTs as the key driver of governance, economy, commerce, trade, and social well-being NORM for: supporting a free and secure internet / cyber space that supports economic growth and innovation
158:1	2014 - Joint+Elements+from+U.S.-EU+Cyber+Dialogue	2014	On the occasion of the inaugural meeting of the U.S.-EU Cyber Dialogue in Brussels, Belgium on December 5, the participants jointly agreed to specific areas of collaboration and cooperation as follows	INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information
158:2	2014 - Joint+Elements+from+U.S.-EU+Cyber+Dialogue	2014	All participants welcomed the landmark consensus of the 2012-2013 Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, including the affirmation of the applicability of existing international law to cyberspace. Both sides welcomed the confidence building measures agreed to in the Organization for Security Cooperation in Europe and their implementation in order to build confidence and reduce the prospects for conflict in cyberspace and commended efforts to expand similar efforts in other regional fora such as the ASEAN Regional Forum and the Organization for American States.	STAKEHOLDER COOPERATION for: support other international and/or regional cooperative partnerships UNITED NATIONS for: following the United Nation's (UN) [2015 and or 2013] GGE report's call for all States to be guided in their use of ICTs in relation to the report
158:3	2014 - Joint+Elements+from+U.S.-EU+Cyber+Dialogue	2014	All reiterated that no single entity, company, organization or government should seek to control the Internet and expressed their full support for multi-stakeholder governance structures of the Internet that are inclusive, transparent, accountable, and technically sound. As such we:	CYBERSPACE STABILITY against: any single entity/company/government/inter-governmental organization should seek control of the internet DIGITAL GOVERNANCE for: future digital [global] governance should be value-based, inclusive, open, and transparent STAKEHOLDER COOPERATION for: coordinate/cooperate in preserving multistakeholder internet governance

ID	Document	Document Groups	Quotation Content	Codes
158:4	2014 - Joint+Elements+from+U.S.-EU+Cyber+Dialogue	2014	emphasized the value of the annual Internet Governance Forum (IGF) and encouraged its ongoing improvements in line with the UN Commission on Science and Technology for Development recommendations. Urged renewal of the IGF's mandate and the continuation of its work, according to paragraph 72 of The Tunis Agenda, beyond the end of its current mandate in 2015.	STATE RESPONSIBILITY for: adhering to rules and regulations agreed upon by previously enacted international law/mandates/treaties
158:5	2014 - Joint+Elements+from+U.S.-EU+Cyber+Dialogue	2014	We affirmed our commitment to promote the Budapest Convention as the reference framework for the fight against cybercrime, including by working together in international fora. We welcome the most recent signatories in 2014: Luxembourg, Turkey, and Panama.	CONFIDENCE BUILDING CBM: adopt legislative basis for combatting cybercrime (i.e., the Budapest Convention)
158:6	2014 - Joint+Elements+from+U.S.-EU+Cyber+Dialogue	2014	They reaffirmed their strong commitment to the promotion and protection of human rights. They emphasized that all human beings have the same human rights online and offline and that states have an obligation to protect those rights in accordance with 3/2/2018 "Joint Elements" from U.S.-EU Cyber Dialogue, 5th December 2014 https://2009-2017.state.gov/r/pa/prs/ps/2014/12/234702.htm 3/3 The Office of Website Management, Bureau of Public Affairs, manages this site as a portal for information from the U.S. State Department. External links to other Internet sites should not be construed as an endorsement of the views or privacy policies contained therein. Note: documents in Portable Document Format (PDF) require Adobe Acrobat Reader 5.0 or higher to view, download Adobe Acrobat Reader (http://get.adobe.com/reader/). international law. In particular, the rights to freedom of expression and privacy, as set out in the International Covenant on Civil and Political Rights, in the digital sphere require the attention of all stakeholders.	HUMAN RIGHTS for: applicability of international human rights law(s) to cyberspace HUMAN RIGHTS for: respecting human rights and fundamental freedoms; applying them to cyber space / ICT use, etc. INDIVIDUAL RIGHTS for: acknowledging that the same rights that individuals have offline are also protected online
158:7	2014 - Joint+Elements+from+U.S.-EU+Cyber+Dialogue	2014	bridging the digital divide towards fostering open societies and enabling economic growth and social development. They reiterated their commitment to an approach to cyber capacity building that leverages the expertise and resources of all stakeholders to ensure that people around the world can fully benefit from the Internet and ICTs. They welcomed further coordination among actors globally and agreed to continue exchanging views and good practices, as well as seeking future synergies in their respective global cyber capacity building initiatives.	CAPACITY BUILDING CBM: encourage further work in capacity-building DIGITAL EQUALITY for: closing the digital divide (i.e., by empowering communities to benefit from digital opportunities) INFORMATION EXCHANGE for: sharing of good/best practices in relation to ICTs and cybersecurity NORM for: promote an open, secure, stable, accessible, and peaceful cyber space / ICT environment
159:1	2014 - Japan-Estonia Summit	2014	On 6 p.m. on March 7, Shinzo Abe, Prime Minister of Japan, held a meeting followed by dinner with H.E. Mr. Thoomas Hendrik Ilves, President of the Republic of Estonia, who made a working visit to Japan upon invitation by the Japanese Government. An outline of the events is as follows:	INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information
159:2	2014 - Japan-Estonia Summit	2014	(1) Prime Minister Abe said threats in cyberspace are matters of security and Japan and Estonia need to make a coordinated response. He also said Japan will formally launch consultations with Estonia on cyber issues and explore cooperation through NATO Cooperative Cyber Defense Centre of Excellence (NATO CCDCOE) based in Estonia.	STAKEHOLDER COOPERATION CBM: states should participate and cooperate in multilateral forums
159:3	2014 - Japan-Estonia Summit	2014	2) In response, President Ilves concurred with the remarks of Prime Minister Abe, including the launch of bilateral consultations on cyberspace issues. He also stated that cyber security is a threat that the international community faces, transcending geographic notions, and Estonia hopes for Japan's cooperation at NATO CCDCOE.	STAKEHOLDER COOPERATION CBM: form bilateral and multilateral cooperation initiatives to build on established partnerships/relationships
160:1	2014 - Wales+Summit+Declaration	2014	Strong partnerships play a key role in addressing cyber threats and risks. We will therefore continue to engage actively on cyber issues with relevant partner nations on a case-by-case basis and with other international organisations, including the EU, as agreed, and will intensify our cooperation with industry through a NATO Industry Cyber Partnership. Technological innovations and expertise from the private sector are crucial to enable NATO and Allies to achieve the Enhanced Cyber Defence Policy's objectives.	STAKEHOLDER COOPERATION CBM: states should participate and cooperate in multilateral forums STAKEHOLDER COOPERATION for: support other international and/or regional cooperative partnerships
160:2	2014 - Wales+Summit+Declaration	2014	We will improve the 3/2/2018 NATO - Official text: Wales Summit Declaration issued by the Heads of State and Government participating in the meeting of the North Atlantic C… https://www.nato.int/cps/en/natohq/official_texts_112964.htm 16/24 level of NATO's cyber defence education, training, and exercise activities	EDUCATION for: increased eduation, [digital] literacy, and awareness regarding digital rights and ways to exercise/protect them STAKEHOLDER COOPERATION for: conduct joint cybersecurity and/or related law enforcement exercises between nation states

ID	Document	Document Groups	Quotation Content	Codes
160:3	2014 - Wales+Summit+Declaration	2014	We, the Heads of State and Government of the member countries of the North Atlantic Alliance, have gathered in Wales at a pivotal moment in Euro-Atlantic security. Russia's aggressive actions against Ukraine have fundamentally challenged our vision of a Europe whole, free, and at peace. Growing instability in our southern neighbourhood, from the Middle East to North Africa, as well as transnational and multi-dimensional threats, are also challenging our security. These can all have long-term consequences for peace and security in the Euro-Atlantic region and stability across the globe	INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information
161:1	2014 - U.S.-Germany Cyber Cyber Dialogue	2014	The Governments of the United States and Germany will hold a Cyber Bilateral Meeting in Berlin, Germany on June 26, 2014.	INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information
161:2	2014 - U.S.-Germany Cyber Cyber Dialogue	2014	This second bilateral engagement follows discussions held on June 14, 2013 in Washington, D.C. that reinforced our alliance by highlighting our collaboration on key cyber issues over the course of the last decade. Prior discussions also embodied a “whole-of- government” approach, furthering U.S. and German cooperation on a wide range of cyber issues and our collaborative engagement on operational and strategic objectives.	STAKEHOLDER COOPERATION CBM: form bilateral and multilateral cooperation initiatives to build on established partnerships/relationships
161:3	2014 - U.S.-Germany Cyber Cyber Dialogue	2014	critical infrastructure protection	CRITICAL INFRASTRUCTURE for: protecting critical infrastructures
161:4	2014 - U.S.-Germany Cyber Cyber Dialogue	2014	combating cybercrime,	STAKEHOLDER COOPERATION for: coordinate/cooperate in combatting cybercrime
162:1	2014 - african_union_convention_on_cyber_security	2014		INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information STAKEHOLDER COOPERATION CBM: states should participate and cooperate in multilateral forums STATE RESPONSIBILITY for: adhering to rules and regulations agreed upon by previously enacted international law/mandates/treaties
162:2	2014 - african_union_convention_on_cyber_security	2014		DOMESTIC LAW for: applicability of domestic law to cyber space / ICT usage HUMAN RIGHTS for: applicability of international human rights law(s) to cyberspace HUMAN RIGHTS for: respecting human rights and fundamental freedoms; applying them to cyber space / ICT use, etc. INTERNATIONAL LAW for: applicability of international law to cyberspace
162:3	2014 - african_union_convention_on_cyber_security	2014		ACCESS for: support the free flow of information while respecting applicable legal frameworks for privacy and data protection CONFIDENCE BUILDING for: ensuring the free flow of data while also protecting the integrity of that data and the privacy of individual users STATE RESPONSIBILITY for: enacting cybersecurity measures that will protect people (privacy, and physical safety, etc) and inform users (transparency)
162:4	2014 - african_union_convention_on_cyber_security	2014		CONFIDENCE BUILDING CBM: voluntary transparency EDUCATION for: increased eduation, [digital] literacy, and awareness regarding digital rights and ways to exercise/protect them PRODUCT CBM: transparency and dialogue regarding ICT vulnerabilities and identified harmful hidden functions in ICT products
162:5	2014 - african_union_convention_on_cyber_security	2014		ACCESS CBM: access to the internet is an important enabler of development./growth/innovation
162:6	2014 - african_union_convention_on_cyber_security	2014		CONFIDENCE BUILDING for: further developement of concepts for international peace and security in the legal use of ICTs (technical and policy level) CRITICAL INFRASTRUCTURE for: protecting critical infrastructures STAKEHOLDER COOPERATION for: coordinate/cooperate in combatting cybercrime

ID	Document	Document Groups	Quotation Content	Codes
162:7	2014 - african_union_convention_on_cyber_security	2014		CONFIDENCE BUILDING CBM: adopt legislative basis for combatting cybercrime (i.e., the Budapest Convention)
162:8	2014 - african_union_convention_on_cyber_security	2014		HUMAN RIGHTS for: applicability of international human rights law(s) to cyberspace HUMAN RIGHTS for: respecting human rights and fundamental freedoms; applying them to cyber space / ICT use, etc.
162:9	2014 - african_union_convention_on_cyber_security	2014		CONFIDENCE BUILDING for: promote the cybersecurity ecosystem STAKEHOLDER COOPERATION for: stakeholders working together on achieving an appropriate balance between the interests of citizens/entities to secure their data, and the needs of law enforcement agencies (while not undermining the fundamentals of technology)
162:10	2014 - african_union_convention_on_cyber_security	2014		STATE RESPONSIBILITY for: dialogue amongst nations by an international body STATE RESPONSIBILITY for: enacting cybersecurity measures that will protect people (privacy, and physical safety, etc) and inform users (transparency) STATE RESPONSIBILITY for: nation-state enacted laws and/or regulations to ensure basic cyber protocols/cleanliness/hygiene STATE RESPONSIBILITY for: protecting transborder critical information infrastructure is a shared responsibility of all States
162:11	2014 - african_union_convention_on_cyber_security	2014		INFORMATION EXCHANGE for: establish a formal framework to facilitate professional dialogue
162:12	2014 - african_union_convention_on_cyber_security	2014		DIGITAL GOVERNANCE for: digital governance must adapt and respond to the needs of citizens STATE RESPONSIBILITY for: timely responses to requests for information
164:1	2014 - IGF Chair Summary	2014	Enhancing Digital Trust Many participants emphasized that there is a need for increased interaction between government entities and all other interested stakeholders in ongoing and future deliberations on enhancing trust in cyberspace.	CONFIDENCE BUILDING for: enhance trust,, confidence, and cooperation regarding ICTs, cyberspace and cybersecurity
164:2	2014 - IGF Chair Summary	2014	Many participants emphasized that there is a need to increase interaction between government entities and all other interested stakeholders in ongoing and future deliberations on enhancing trust in cyberspace.	STAKEHOLDER COOPERATION CBM: cooperation between states/entities (domestic and/or international) is important for furthering economic relationships/development STAKEHOLDER COOPERATION CBM: form bilateral and multilateral cooperation initiatives to build on established partnerships/relationships STAKEHOLDER COOPERATION CBM: states should participate and cooperate in multilateral forums STAKEHOLDER COOPERATION for: coordinate/cooperate in preserving multistakeholder internet governance

ID	Document	Document Groups	Quotation Content	Codes
164:3	2014 - IGF Chair Summary	2014	WSIS+10 High-Level Event Information Session This session on the World Summit on the Information Society High-level Event, organized by the ITU, provided an opportunity for the IGF community to learn more about the outcomes of the event and its implications for the ongoing UN General Assembly WSIS+10 review process. CSTD Ten-year Review of WSIS The United Nations Conference on Trade and Development (UNCTAD), which performs the CSTD secretariat function, is currently facilitating the CSTD's ten-year review of the progress made in the implementation of the WSIS outcomes, as mandated by the Economic and Social Council. UNCTAD encouraged IGF participants to contribute to through an online questionnaire at http://unctad.org/en/Pages/CSTD/WSIS-10yearReview.aspx by the deadline, 15 September 2014. UNESCO's Comprehensive Study on the Internet The United Nations Educational, Scientific and Cultural Organization asked stakeholders in Istanbul to contribute to its Internet study which covers issues related to access to information and knowledge, freedom of expression, privacy, and ethical dimensions of the information society. UNESCO encouraged all IGF participants to contribute to the study, which is open for comments until 30 November 2014. The study is available at http://www.unesco.org/new/en/communication-and-information/crosscutting- priorities/unesco-internet· study. African Declaration on Internet Rights and Freedoms The declaration, which is a Pan-African initiative to promote human rights standards and openness principles in Internet-policy making on the continent, was launched at the 2014 IGF. The declaration is available at http://africaninternetrights.org. Dynamic Coalition on Accessibility and Disability (DCAD) Accessibility Guidelines The Internet Governance Forum's Dynamic Coalition on Accessibility and Disability (DCAD) approved and formally submitted a set of guidelines, "DCAD Accessibility Guidelines 2014: Accessibility and Disability in IGF meetings". The guidelines outline how to improve accessibility at IGF meetings and to eliminate barriers for participants with disabilities. The intention is to help the IGF Secretariat to improve accessibility for persons with disabilities and to encourage and facilitate their participation in IGF meetings. The document was formally presented during the Taking Stock main/focus session as an output document of the ninth IGF meeting. The guidelines are available at http://www.intgovforum.org/cms/documents/dynamic-coalitions/dynamic-coalition-on- accessibility-	STAKEHOLDER COOPERATION for: support other international and/or regional cooperative partnerships STATE RESPONSIBILITY for: adhering to rules and regulations agreed upon by previously enacted international law/mandates/treaties
164:4	2014 - IGF Chair Summary	2014	Participants discussed during the wrap-up session some of the problems with using the term "best practices" and came to an agreement that the IGF process moving forward could use instead "best practices to date" or "lessons learned to date". This will reflect that the IGF needs to be very forward-looking and very flexible in the development of any recommendation for best practices, because those will continue to evolve with the Internet. There was also agreement that to make the exercise more effective, there is a need for both more time and more resources to support the efforts. The process definitely needs to be an iterative collaborative process, working for consensus, not negotiating final outcome text. Finally there was also agreement that in the future there needs to be more effort to understand the situation in developing countries, what kind of practices would be useful to people from those countries, and also to bring in youth.	ASSIST for: adopting appropriate policies and measures so that developing countries benefit from the advantages of technological progress (and do not suffer from lack of early adoption) ASSISTANCE CBM: provide assistance and training to developing countries to improve cybsecurity and ICT use INFORMATION EXCHANGE for: sharing of good/best practices in relation to ICTs and cybersecurity
164:5	2014 - IGF Chair Summary	2014	Roundtable participants recognised the maturity on discussions of human rights at the IGF. In particular, the work of the Internet Rights and Principles Dynamic Coalition, and the increasing number of workshops on the topic at the IGF were mentioned. It was also underlined that maturity of the discussions at the IGF contributed to make human rights a central principle of the NETmundial Multistakeholder Statement of Sao Paulo. Participants also recommended the creation of a new best practice forum at the IGF on the issue of protection of privacy in the digital age. It was proposed that prior to the IGF 2015 in Brazil, a process could arrive at some definitional clarity as well as capture good practices on the protection of privacy in the digital age. This inter-sessional process needs to include developing country participation and make use of regional and national IGFs to ensure that such inclusion happens	ACCESS for: support the free flow of information while respecting applicable legal frameworks for privacy and data protection CONFIDENCE BUILDING for: ensuring the free flow of data while also protecting the integrity of that data and the privacy of individual users HUMAN RIGHTS for: respecting human rights and fundamental freedoms; applying them to cyber space / ICT use, etc. STATE RESPONSIBILITY for: enacting cybersecurity measures that will protect people (privacy, and physical safety, etc) and inform users (transparency)

ID	Document	Document Groups	Quotation Content	Codes
164:6	2014 - IGF Chair Summary	2014	Feminist Principles of the Internet The Association for Progressive Communications (APC) launched the document, “Feminist Principles of the Internet”, at the Sex, Rights and Internet Governance pre-event. The document lists 15 principles that assert feminist views on positions related to Internet and communication rights, including privacy and surveillance, diverse and inclusive participation in decision-making, open source technology, regulation of sexual content and online pornography. The drafting of the principles began at a global meeting in April 2014 and were continued online via Twitter, using the hashtag #ImagineaFeministInternet, in the lead up to IGF 2014. Feedback and comments from stakeholders from the document is encouraged by the developers of the document at http://www.genderit.org/articles/feminist-principles-internet.	DIGITAL EQUALITY CBM: work towards digital equality and inclusion (i.e., for women and traditionally marginalised groups) - this includes cooperation between the private sector, civil society, and national governments (as well as multilateral banks, and international entities such as the United Nations) DIGITAL EQUALITY for: closing the gender digital divide (focusing on women and girls, but also those a part of gender subgroups such as the LGBTQI+ communiy)
164:7	2014 - IGF Chair Summary	2014	Policies Enabling Access, Growth and Development on the Internet To facilitate the connection of the next five billion currently not connected, a strong call was made for an increased emphasis and inclusion of ICTs and Internet access in the post-2015 development agenda of the UN, as a catalyst for economic growth.	UNITED NATIONS CBM: the United Nations (UN) may serve as an international body for decision-making, framework creation/implementation, and when developing and adopting universally agreed upon ICT norms/rules/principles (in order to ensure peace and responsible behavior/ICT use) UNITED NATIONS for: following the United Nation's (UN) [2015 and or 2013] GGE report's call for all States to be guided in their use of ICTs in relation to the report
165:1	2014 - International Cybersecurity Norms	2014	Norms for improving defenses, which can reduce risk by providing a foundation for national cybersecurity capacity and for domestic, regional, and international organizational structures and approaches that increase understanding between states • Norms for limiting conflict or offensive operations, which will serve to reduce conflict, avoid escalations, and limit the potential for catastrophic impacts in, through, or even to cyberspace	CRITICAL INFRASTRUCTURE for: promoting resilience (as related to ICTs,cybersecurity, and related critical infrastructure
165:2	2014 - International Cybersecurity Norms	2014	• Offensive cyber operations as state or state-sponsored actions, such as theft or manipulation of data, and tampering with the integrity of private sector products, services, and operations. • Cyber weapons as a combination of information systems, programs, or data designed, equipped, or modified to destroy, disrupt, or corrupt critical physical or information cyber infrastructure.	CRITICAL INFRASTRUCTURE for: protecting critical infrastructures CYBER ATTACK for: preventing ICT-enabled theft of intellectual property (this includes trade secrets and other confidential business information) PRODUCT TAMPERING against: states and non-state actors tampering with products/services (knowingly inserting harmful material into their products) NOR allowing their products to be tampered with PRODUCT TAMPERING for: rejecting any apparent state or non-state efforts to compromise products/services STATE RESPONSIBILITY & SOVEREIGNTY against: conducting or supporting ICT-enabled theft of intellectual property, trade secrets, or other confidential business info TAMPERING for: adopt practices that reduce the risk of tampering as well as permit response if tampering is discovered
165:3	2014 - International Cybersecurity Norms	2014	NORM 1: States should not target ICT companies to insert vulnerabilities (backdoors) or take actions that would otherwise undermine public trust in products and services.	STATE RESPONSIBILITY against: targeting global ICT companies in order to insert vulnerabilities (backdoors) or take actions that would otherwise undermine public trust in products and services
165:4	2014 - International Cybersecurity Norms	2014	NORM 2: States should have a clear principle-based policy for handling product and service vulnerabilities that reflects a strong mandate to report them to vendors rather than to stockpile, buy, sell, or exploit them	DIGITAL ECONOMY for: states are responsible to notify ICT supply chain/product users when significant vulnerabilities are identified PRODUCT CBM: transparency and dialogue regarding ICT vulnerabilities and identified harmful hidden functions in ICT products PRODUCT for: creating transparent procedures and frameworks to asses whether and when to disclose not publicly known vulnerabilities or flaws in their information systems and/or technologies PRODUCT for: developers and producers of products and services should take measures to timely mitigate vulnerabilities that are later discovered and be transparent about their process PRODUCT for: developers and producers of products and services should take reasonable steps to ensure that their products/services are free from significant vulnerabilities
165:5	2014 - International Cybersecurity Norms	2014	NORM 4: States should commit to nonproliferation activities related to cyber weapons. As states increase investments in offens	STATE RESPONSIBILITY for: commit to nonproliferation activities related to cyber weapons

ID	Document	Document Groups	Quotation Content	Codes
165:6	2014 - International Cybersecurity Norms	2014	NORM 6: States should assist private sector efforts to detect, contain, respond to, and recover from events in cyberspace.	CYBER ATTACKS for: responding to requests for help in the event of a cyber attack CYBER ATTACKS for: strengthen tools and resources needed to prepare, deter, defend, and respond to unlawful use of ICTs, cyber attacks / acts of cyber crime and/or terrorism
165:7	2014 - International Cybersecurity Norms	2014	In efforts to improve cybersecurity, the need for multiple stakeholders is an operational reality rather than an ideology. The development of cybersecurity norms cannot be a niche foreign policy issue reserved for diplomats. Cybersecurity norms are an imperative for all users, governments, the private sector, non-governmental organizations (NGOs), and individuals, in an Internet-dependent world—each contributes to the peace, security, and sustained innovation of a globally interconnected society. These stakeholders can and should contribute their expertise to the norm development process, acknowledging that all stakeholders may not be equal partners in every effort due to different levels of expertise. Developing soft norms that gradually morph into customary international law will allow for strong input by the private sector, academia, and civil society. Law-making or adoption of potential treaties, however, should remain the prerogative of governments and subject to national political processes.	STAKEHOLDER COOPERATION for: coordinate/cooperate in preserving multistakeholder internet governance
165:8	2014 - International Cybersecurity Norms	2014	• Bilateral consultations. Many countries have set up bilateral consultations on cyberspace. This work is important, since it drives increased transparency around state behavior in cyberspace, as countries begin to identify relevant structures and to share contact lists and (military/national security) doctrine. However, as previously outlined, bilateral consultations alone are not sufficient to increase the stability and resilience of cyberspace. Moreover, it is often the case that private sector owners and operators of the impacted ICTs and civil society don't often get invited to such dialogue. Although many governments are confident in their ability to manage regulated telecommunications infrastructure in international negotiations, cyberspace is different—with software and services that are often not as clearly bound to geographic location.	STAKEHOLDER COOPERATION CBM: form bilateral and multilateral cooperation initiatives to build on established partnerships/relationships
165:9	2014 - International Cybersecurity Norms	2014	• Regional approaches. In developing new norms of behavior, another option is to leverage existing dialogues in this space. One example could be building on the debate on the Network and Information Security (NIS) Directive13in the European Union and extending the dialogue to international norms, first in Europe and then internationally. The similar focus of the NIS Directive and the Cybersecurity Framework14on cyber risk management and on protecting critical infrastructures in the United States provides opportunities for alignment. Building on those efforts to extend the normative behavior of the critical infrastructure to other regions around the world would be a meaningful step. • G20 + ICT20. A third option could be leveraging existing frameworks, such as G20, and extending them to 20 leading ICT providers (ICT20). The G20 + ICT20 would have the advantage of being global in nature yet manageable in terms of size. An agreed-upon norms document between these stakeholders could represent a powerful contribution to a first cybersecurity norms baseline. It would also allow the 20 most developed economies to hold themselves and others accountable to the agreed-upon behaviors in cyberspace. The drawback of such a group is its lack of truly global	STAKEHOLDER COOPERATION CBM: states should participate and cooperate in multilateral forums STAKEHOLDER COOPERATION for: support other international and/or regional cooperative partnerships
167:1	2013 - Summary of chairman IGF 2013	2013	The various sub-themes for the 8th IGF included: Access and Diversity - Internet as an Engine for Growth and Sustainable Development; Openness - Human rights, Freedom of Expression and Free Flow of Information on the Internet; Security - Legal and other Frameworks: Spam, Hacking and Cyber-crime; Enhanced Cooperation; Principles of Multistakeholder Cooperation and Internet Governance Principles. 135 focus sessions, workshops, open forums, flash sessions and other meetings took place over the 4 day event.	ACCESS for: support the free flow of information while respecting applicable legal frameworks for privacy and data protection CONFIDENCE BUILDING for: ensuring the free flow of data while also protecting the integrity of that data and the privacy of individual users HUMAN RIGHTS for: respecting human rights and fundamental freedoms; applying them to cyber space / ICT use, etc. STAKEHOLDER COOPERATION for: coordinate/cooperate in combatting cybercrime STAKEHOLDER COOPERATION for: coordinate/cooperate in preserving multistakeholder internet governance

ID	Document	Document Groups	Quotation Content	Codes
167:2	2013 - Summary of chairman IGF 2013	2013	H.E. Tifatul Sembiring, Minister of Communications and Information Technology (MCIT), of the Republic of Indonesia, who assumed the chairmanship of the meeting, welcomed all participants to Indonesia and the island of Bali and explained that with more than 63 million Internet users already in Indonesia, making the Internet available to the people was not the only goal his government hopes to achieve. They are committed to making sure that the Internet is both affordable and accessible throughout the nation, particularly in the rural areas. Participants were also reminded that increased connectivity also brings unique security challenges. Individual	ACCESS CBM: access to the internet is an important enabler of development./growth/innovation
167:3	2013 - Summary of chairman IGF 2013	2013	and trust in the use of the Internet so that cyber technology may bring us progress, peace and prosperity	NORM for: promote an open, secure, stable, accessible, and peaceful cyber space / ICT environment
167:4	2013 - Summary of chairman IGF 2013	2013	The first part of the Focus dialogue examined spam and its emerging challenges and opportunities for capacity building to exchange expertise on mitigation and prevention with countries and communities who are interested in establishing spam mitigation initiatives. Participants in the meeting and following remotely examined the roles that the multistakeholder community plays in possible technical solutions and examples of sound regulatory approaches, need for legal frameworks and law enforcement responses that are necessary to address the growing issue of spam in particular in Developing countries. There was consensus of the participants that while spam may be ill defined as unwanted or unsolicited electronic communication or email, it is the delivery mechanism whereby malware, botnets and phishing attacks infect unsuspecting users. Cooperation amongst all responsible actors for prevention of such acts as well as the importance of public private partnerships and cross-border synergy amongst governments, the technical community, the private sector and law enforcement was noted in the work being performed in industry groups. The work of the Internet Society"s Combating Spam Project to bring together technical experts and organizations such as MAAWG, the London Action Plan and within the GSMA to work with Developing countries to address from a global perspective the ever-shifting nature of spam attacks.	STAKEHOLDER COOPERATION for: coordinate/cooperate in combatting cybercrime STATE RESPONSIBILITY for: adhering to rules and regulations agreed upon by previously enacted international law/mandates/treaties
167:5	2013 - Summary of chairman IGF 2013	2013	The Messaging Anti-Abuse Working Group (MAAWG) and the London Action Plan (LAP) were both mentioned as strong multistakeholder global initiatives that are working actively on prevention measures for harmful activities on the web. The Budapest Convention on Cyber-Crime was also said to be a strong starting point and groundwork for international cooperation efforts	CONFIDENCE BUILDING CBM: adopt legislative basis for combatting cybercrime (i.e., the Budapest Convention)
167:6	2013 - Summary of chairman IGF 2013	2013	Many emphasized the need to strike a balance between keeping the Internet both open and secure. Efforts to secure networks should not stifle innovation by fragmenting network flows of information. The IGF is the ideal forum for further debates and discussions on issues related to spam, hacking and cyber-crime because of its inherent multistakeholder nature.	STAKEHOLDER COOPERATION for: coordinate/cooperate in preserving multistakeholder internet governance
169:1	2013 - Japan-U.S. Cyber Dialogue	2013	The Governments of Japan and the United States held the first Japan-U.S. Cyber Dialogue in Tokyo on May 9-10, 2013.	INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information
169:2	2013 - Japan-U.S. Cyber Dialogue	2013	consultation for exchanging cyber threat information, aligning international cyber policies, comparing national cyber strategies, cooperating on planning and efforts to protect critical infrastructure, and discussing the cooperation on cyber areas in national defense and security policy.	CRITICAL INFRASTRUCTURE for: protecting critical infrastructures
169:3	2013 - Japan-U.S. Cyber Dialogue	2013	Affirming common objectives in international cyber fora, especially the application of norms of responsible state behavior in cyberspace	NORMS CBM: universally agreed upon [voluntary] norms/rules/principles are important for the responsible behavior of States' use of ICTs
169:4	2013 - Japan-U.S. Cyber Dialogue	2013	Supporting the development of practical confidence-building measures and the implementation of national whole-of-government cyber strategies in an effort to reduce risk in cyberspace	CONFIDENCE BUILDING for: develop and implement [practical] cyber confidence building measures (CBMs) between nation states
169:5	2013 - Japan-U.S. Cyber Dialogue	2013	Confirming support for the preservation of openness and interoperability enhanced by the multi-stakeholder system of Internet governance.	STAKEHOLDER COOPERATION for: coordinate/cooperate in preserving multistakeholder internet governance
169:6	2013 - Japan-U.S. Cyber Dialogue	2013	Coordinating cooperation on cyber capacity-building efforts in third countries.	ASSISTANCE CBM: provide assistance and training to developing countries to improve cybsecurity and ICT use
169:7	2013 - Japan-U.S. Cyber Dialogue	2013	Addressing the increasing role of cyber defense in national defense and security strategies and discussing new areas of bilateral cyber defense cooperation.	STAKEHOLDER COOPERATION CBM: form bilateral and multilateral cooperation initiatives to build on established partnerships/relationships

ID	Document	Document Groups	Quotation Content	Codes
170:1	2013 - BRICS eThekwini Declaration	2013	We, the leaders of the Federative Republic of Brazil, the Russian Federation, the Republic of India, the People's Republic of China and the Republic of South Africa, met in Durban, South Africa, on 27 March 2013 at the Fifth BRICS Summit. Our discussions took place under the overarching theme, "BRICS and Africa: Partnership for Development, Integration and Industrialisation". The Fifth BRICS Summit concluded the first cycle of BRICS Summits and we reaffirmed our commitment to the promotion of international law, multilateralism and the central role of the United Nations (UN). Our discussions reflected our growing intra-BRICS solidarity as well as our shared goal to contribute positively to global peace, stability, development and cooperation. We also considered our role in the international system as based on an inclusive approach of shared solidarity and cooperation towards all nations and peoples.	INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information INTERNATIONAL LAW for: applicability of international law to cyberspace STAKEHOLDER COOPERATION CBM: states should participate and cooperate in multilateral forums STATE RESPONSIBILITY for: adhering to rules and regulations agreed upon by previously enacted international law/mandates/treaties UNITED NATIONS CBM: the United Nations (UN) may serve as an international body for decision-making, framework creation/implementation, and when developing and adopting universally agreed upon ICT norms/rules/principles (in order to ensure peace and responsible behavior/ICT use)
170:2	2013 - BRICS eThekwini Declaration	2013	We recognize the critical positive role the Internet plays globally in promoting economic, social and cultural developmen	CONFIDENCE BUILDING CBM: recognize importance of ICTs as the key driver of governance, economy, commerce, trade, and social well-being NORM for: supporting a free and secure internet / cyber space that supports economic growth and innovation
170:3	2013 - BRICS eThekwini Declaration	2013	We believe it's important to contribute to and participate in a peaceful, secure, and open cyberspace and we emphasise that security in the use of Information and Communication Technologies (ICTs) through universally accepted norms, standards and practices is of paramount importance.	NORM for: promote an open, secure, stable, accessible, and peaceful cyber space / ICT environment NORMS CBM: universally agreed upon [voluntary] norms/rules/principles are important for the responsible behavior of States' use of ICTs
171:1	2013 - Initial+Set+of+OSCE+Confidence-Building+Measures	2013	The OSCE participating States, recalling the OSCE role as a regional arrangement under Chapter VIII of the UN Charter, confirm that the CBMs being elaborated in the OSCE complement UN efforts to promote CBMs in the field of security of and in the use of ICTs. The efforts of the OSCE participating States in implementation of the OSCE confidence-building measures in the field of security of and in the use of ICTs will be consistent with: international law, including, inter alia, the UN Charter and the International Covenant on Civil and Political Rights; as well as the Helsinki Final Act; and their responsibilities to respect human rights and fundamental freedoms.	HUMAN RIGHTS for: respecting human rights and fundamental freedoms; applying them to cyber space / ICT use, etc. STATE RESPONSIBILITY for: adhering to rules and regulations agreed upon by previously enacted international law/mandates/treaties
171:2	2013 - Initial+Set+of+OSCE+Confidence-Building+Measures	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.	INFORMATION EXCHANGE CBM: exchange national views on the use of ICTS in conflicts
171:3	2013 - Initial+Set+of+OSCE+Confidence-Building+Measures	2013	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	INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information
171:4	2013 - Initial+Set+of+OSCE+Confidence-Building+Measures	2013	articipating States will on a voluntary basis and at the appropriate level hold consultations in order to reduce the risks of misperception, and of possible emergence of political or military tension or conflict that may stem from the use of ICTs, and to protect critical national and international ICT infrastructures including their integrity	CRITICAL INFRASTRUCTURE for: protecting critical infrastructures STATE RESPONSIBILITY CBM: transnational consulting to reduce risk of misperception, escalation, and conflict
171:5	2013 - Initial+Set+of+OSCE+Confidence-Building+Measures	2013	he participating States will use the OSCE as a platform for dialogue, exchange of best practices, awareness-raising and information on capacity-building regarding security of and in the use of ICTs, including effective responses to related threats. The participating States will explore further developing the OSCE role in this regard.	INFORMATION EXCHANGE for: sharing of good/best practices in relation to ICTs and cybersecurity STATE RESPONSIBILITY for: dialogue amongst nations by an international body
171:6	2013 - Initial+Set+of+OSCE+Confidence-Building+Measures	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. The OSCE participating States agree that the OSCE shall not duplicate the efforts of existing law enforcement channels.	STAKEHOLDER COOPERATION CBM: form bilateral and multilateral cooperation initiatives to build on established partnerships/relationships STAKEHOLDER COOPERATION for: conduct joint cybersecurity and/or related law enforcement exercises between nation states

ID	Document	Document Groups	Quotation Content	Codes
172:1	2013 - U.S.-Germany Cyber Bilateral Meeting	2013	The text of the following statement was agreed by the Governments of the United States of America and the Federal Republic of Germany on the occasion of the U.S.-Germany Cyber Bilateral Meeting June 10-11, 2013.	INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information
172:2	2013 - U.S.-Germany Cyber Bilateral Meeting	2013	The U.S.-Germany Cyber Bilateral Meeting reinforced our long-standing alliance by highlighting our pre-existing collaboration on many key cyber issues over the course of the last decade and identifying additional areas for awareness and alignment. The U.S.- Germany Cyber Bilateral Meeting embodied a “whole-of-government” approach, furthering our cooperation on a wide range of cyber issues and our collaborative engagement on both operational and strategic objectives.	STAKEHOLDER COOPERATION CBM: form bilateral and multilateral cooperation initiatives to build on established partnerships/relationships
172:3	2013 - U.S.-Germany Cyber Bilateral Meeting	2013	combating cybercrime, developing practical confidence-building measures to reduce risk, and exploring new areas of bilateral cyber defense cooperation.	CONFIDENCE BUILDING for: develop and implement [practical] cyber confidence building measures (CBMs) between nation states STAKEHOLDER COOPERATION for: coordinate/cooperate in combatting cybercrime
172:4	2013 - U.S.-Germany Cyber Bilateral Meeting	2013	common cyber approaches in Internet governance, Internet freedom, and international security; partnering with the private sector to protect critical infrastructure, including through prospective legislation and other frameworks; and pursuing coordination efforts on cyber capacity-building in third countries. The discussions specifically focused on continued and bolstered support for the multi-stakeholder model for Internet governance,	ASSISTANCE CBM: provide assistance and training to developing countries to improve cybsecurity and ICT use HUMAN RIGHTS for: respecting human rights and fundamental freedoms; applying them to cyber space / ICT use, etc. STAKEHOLDER COOPERATION for: coordinate/cooperate in preserving multistakeholder internet governance STAKEHOLDER COOPERATION for: recognizing the private sector's responsibilities in working towards improving trust, security, and stability in cyberspace
172:5	2013 - U.S.-Germany Cyber Bilateral Meeting	2013	and the application of norms and responsible state behavior in cyberspace, particularly next steps in light of successful UN Group of Governmental Experts consensus where key governmental experts affirmed the applicability of international law to state behavior in cyberspace.	INTERNATIONAL LAW for: applicability of international law to cyberspace UNITED NATIONS for: following the United Nation's (UN) [2015 and or 2013] GGE report's call for all States to be guided in their use of ICTs in relation to the report
172:6	2013 - U.S.-Germany Cyber Bilateral Meeting	2013	Germany noted its concern in connection with the recent disclosures about U.S. Government surveillance programs. The U.S. referenced statements by the U.S. President and the Director of National Intelligence on this issue and emphasized that such programs are designed to protect the United States and other countries from terrorist and other threats, are consistent with U.S. law, and are subject to strict supervision and oversight by all three branches of the U.S. Government. Both sides recognized that this issue will be the subject of further dialogue.	DOMESTIC LAW for: applicability of domestic law to cyber space / ICT usage
173:1	2013 - EU+Council+Conclusions+on+ Cybersecurity	2013	he critical importance of a vibrant EU Information and Communication Technology (ICT) and ICT Security Sector with regards to the reinforcement of cybersecurity and INVITES Member States and the Commission to explore and report on what steps can be taken to support its development,	CRITICAL INFRASTRUCTURE for: protecting critical infrastructures
173:2	2013 - EU+Council+Conclusions+on+ Cybersecurity	2013	to support awareness-raising on the nature of the threats and the fundamentals of good digital practices, at all levels,	EDUCATION for: implementing [community] education and awareness in order to prevent cybercrime EDUCATION for: increased eduation, [digital] literacy, and awareness regarding digital rights and ways to exercise/protect them
173:3	2013 - EU+Council+Conclusions+on+ Cybersecurity	2013	to foster pan-European cybersecurity cooperation, in particular by enhancing pan- European cybersecurity exercises,	STAKEHOLDER COOPERATION for: conduct joint cybersecurity and/or related law enforcement exercises between nation states STAKEHOLDER COOPERATION for: support other international and/or regional cooperative partnerships
173:4	2013 - EU+Council+Conclusions+on+ Cybersecurity	2013	to engage with industry and academia to stimulate trust as a key component of national cybersecurity for instance by setting up public-private partnerships	CONFIDENCE BUILDING CBM: further investments in ICT research and development INFORMATION EXCHANGE CBM: encourage further analysis and study by research institutes and universities on ICT security related matters INFORMATION EXCHANGE CBM: encouraging exchanges between research and academic institutions
173:5	2013 - EU+Council+Conclusions+on+ Cybersecurity	2013	to ensure effective cooperation and coordination between Member States at EU level, towards a common threats' assessment,	STAKEHOLDER COOPERATION CBM: states should participate and cooperate in multilateral forums

ID	Document	Document Groups	Quotation Content	Codes
173:6	2013 - EU+Council+Conclusions+on+ Cybersecurity	2013	INVITES the Member States, the Commission and ENISA to strengthen efforts on Research and Development in the area of ICT and cybersecurity, as well as the availability of well- prepared professionals on cybersecurity, essential to boost the competitiveness of the European Information and Communication Technology (ICT), service and security industries, and their ability to develop trustworthy and secure solutions, hence the Council ENCOURAGES the Commission to leverage the Horizon 2020 Framework Programme for Research and Innovation	STATE RESPONSIBILITY for: adhering to rules and regulations agreed upon by previously enacted international law/mandates/treaties
173:7	2013 - EU+Council+Conclusions+on+ Cybersecurity	2013	in cooperation with Member States and relevant private organisations and civil society to make full use of relevant EU aid instruments for ICT capacity building, including cybersecurity	CAPACITY BUILDING CBM: develop regional approaches to capacity-building CAPACITY BUILDING CBM: encourage further work in capacity-building
173:8	2013 - EU+Council+Conclusions+on+ Cybersecurity	2013	supporting capacity-building in third countries, through training and assistance for the creation of relevant national policies, strategies and institutions, in view of enabling the full economic and social potential of ICTs, supporting the development of resilient systems in those countries and mitigating cyber risks for the EU institutions and Member States, while making use of existing networks and forums for policy coordination and information exchange.	ASSISTANCE CBM: provide assistance and training to developing countries to improve cybsecurity and ICT use
173:9	2013 - EU+Council+Conclusions+on+ Cybersecurity	2013	Open-ended informal OSCE working group to elaborate a set of draft confidence- building measures CBM's to enhance interstate cooperation, transparency, predictability, and stability, and to reduce the risks of misperception, escalation and conflict that may stem form the use of ICTs (OCSE perm. Council decision no. 1039, 26 April 2012)	CONFIDENCE BUILDING CBM: CBM are important for increasing transparency, predictability, and stability CONFIDENCE BUILDING for: develop and implement [practical] cyber confidence building measures (CBMs) between nation states NORM for: promote an open, secure, stable, accessible, and peaceful cyber space / ICT environment
173:10	2013 - EU+Council+Conclusions+on+ Cybersecurity	2013	UNDERLINING the roles and rights of individual citizens, the private sector, and civil society in cyber issues and the important role of the EU in supporting and maintaining an open, secure and resilient cyberspace based on the core values of the EU such as democracy, human rights, and the rule of law, for our economies, administrations and society and for the smooth functioning of the internal marke	HUMAN RIGHTS for: applicability of international human rights law(s) to cyberspace HUMAN RIGHTS for: respecting human rights and fundamental freedoms; applying them to cyber space / ICT use, etc. NORM for: supporting a free and secure internet / cyber space that supports economic growth and innovation STAKEHOLDER COOPERATION for: stakeholders working together on achieving an appropriate balance between the interests of citizens/entities to secure their data, and the needs of law enforcement agencies (while not undermining the fundamentals of technology)
173:11	2013 - EU+Council+Conclusions+on+ Cybersecurity	2013	RECOGNISING that international law, including international conventions such as the Council of Europe Convention on Cybercrime (Budapest Convention) and relevant conventions on international humanitarian law and human rights, such as the International Covenant on Civil and Political Rights, the International Covenant on Economic, Social and Cultural Rights provide a legal framework applicable in cyberspace. Efforts should therefore be made to ensure that these instruments are upheld in cyberspace; therefore the EU does not call for the creation of new international legal instruments for cyber issue	CONFIDENCE BUILDING CBM: adopt legislative basis for combatting cybercrime (i.e., the Budapest Convention)
173:12	2013 - EU+Council+Conclusions+on+ Cybersecurity	2013	reflects the roles and rights of individual citizens, the private sector, and civil society in cyber issues; including a strengthening of public-private cooperation and exchange of information,	STAKEHOLDER COOPERATION for: encourage participation of other stakeholders such as the private sector, academia, and civil society orgs (as appropriate) for CBM and/or norm creation and implementation STAKEHOLDER COOPERATION for: work with states and/or the private sector/civil society (international and/or domestic) to further cooperate on topics such as law enforcement, prosecution, investment, e-commerce, intellectual property rights, etc.
174:1	2013 - 12th Meeting of Foreign Ministers of Russia-India-China	2013	The Foreign Ministers of the Republic of India, the Russian Federation and the People's Republic of China met in New Delhi on 10 November 2013 for their 12th Meeting. The meeting was held in an atmosphere marked with cordiality and warmth.	INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information

ID	Document	Document Groups	Quotation Content	Codes
174:2	2013 - 12th Meeting of Foreign Ministers of Russia-India-China	2013	The Ministers expressed concern at the growing threat of the use of information and communication technologies for criminal and terrorist purposes, as well as for purposes that are inconsistent with the UN Charter.They reiterated that it is important to contribute to and participate in a peaceful, secure, and open cyberspace and emphasized that security in the use of Information and Communication Technologies (ICTs) through universally accepted norms, standards and practices is of paramount importance.	CYBER ATTACKS for: strengthen tools and resources needed to prepare, deter, defend, and respond to unlawful use of ICTs, cyber attacks / acts of cyber crime and/or terrorism NORMS CBM: universally agreed upon [voluntary] norms/rules/principles are important for the responsible behavior of States' use of ICTs STAKEHOLDER COOPERATION for: coordinate/cooperate in combatting cybercrime STAKEHOLDER COOPERATION for: work / intensify cooperation against criminal/terrorist use of ICTs STATE RESPONSIBILITY for: adhering to rules and regulations agreed upon by previously enacted international law/mandates/treaties
174:3	2013 - 12th Meeting of Foreign Ministers of Russia-India-China	2013	The Ministers considered the UN to be the foremost multilateral forum entrusted with bringing about hope, peace and sustainable development to the world. They expressed strong commitment to multilateral diplomacy with the United Nations playing the leading role in dealing with global challenges and threats. In this context, they reafrmed the need for a comprehensive reform of the UN, including its Security Council, with a view to making it more efective, efcient and representative, so that it can deal with today's global challenges more successfully	UNITED NATIONS CBM: the United Nations (UN) may serve as an international body for decision-making, framework creation/implementation, and when developing and adopting universally agreed upon ICT norms/rules/principles (in order to ensure peace and responsible behavior/ICT use)
174:4	2013 - 12th Meeting of Foreign Ministers of Russia-India-China	2013	The Ministers reiterated the importance attached by their countries to cooperation within BRICS. In this context, they reafrmed their determination to work together to further strengthen BRICS as a mechanism for consultation, coordination and cooperation on global and regional political and economic issues of mutual interests. 22. The Foreign Ministers of China and Russia supported India's active engagement with and positive contributions to the Shanghai Cooperation Organization. 23. The Ministers stressed the need to develop an open, inclusive and transparent security architecture in the Asia Pacifc region based upon universally agreed principles of international law. They underscored the importance of the East Asia Summit as a forum for dialogue and cooperation on broad strategic, political and economic issues of common interest with the aim of promoting peace, stability and economic prosperity in East Asia. They underlined the necessity to further strengthen coordination and cooperation in various regional fora such as the ASEAN Regional Forum (ARF), ASEAN Defense Ministers Plus (ADMM-Plus), Asia-Europe Meeting (ASEM), Shanghai Cooperation Organization (SCO), Conference on Interaction and Confdence Building Measures in Asia (CICA) and Asia Cooperation Dialogue (ACD).India and Russia expressed their support to China for hosting the CICA Summit in 2014.	STAKEHOLDER COOPERATION for: support other international and/or regional cooperative partnerships
175:1	2013 - U.S.-Russian+Cooperation	2013	The United States and the Russian Federation have also concluded a range of steps designed to increase transparency and reduce the possibility that a misunderstood cyber incident could create instability or a crisis in our bilateral relationship. Taken together, they represent important progress by our two nations to build confidence and strengthen our relations in cyberspace; expand our shared understanding of threats appearing to emanate from each other’s territory; and prevent unnecessary escalation of ICT security incidents.	INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information STAKEHOLDER COOPERATION CBM: form bilateral and multilateral cooperation initiatives to build on established partnerships/relationships STATE RESPONSIBILITY CBM: transnational consulting to reduce risk of misperception, escalation, and conflict
175:2	2013 - U.S.-Russian+Cooperation	2013	To facilitate the regular exchange of practical technical information on cybersecurity risks to critical systems, we are arranging for the sharing of threat indicators between the U.S. Computer Emergency Readiness Team (US-CERT), located in the Department of Homeland Security, and its counterpart in Russia. On a continuing basis, these two authorities will exchange technical information about malware or other malicious indicators, appearing to originate from each other’s territory, to aid in proactive mitigation of threats. This kind of exchange helps expand the volume of technical cybersecurity information available to our countries, improving our ability to protect our critical networks.	CRITICAL INFRASTRUCTURE for: protecting critical infrastructures EMERGENCY RESPONSE CBM: assist in strengthening cooperation amongst national computer ER teams etc. EMERGENCY RESPONSE CBM: create procedures for mutual assistance in times of incident response EMERGENCY RESPONSE CBM: develop guidance in order to exchange lessons on establishing and exercising secure crisis communication channels STATE RESPONSIBILITY & SOVEREIGNTY for: ensuring that one's territory is not used by non-State actors to commit internationally wrongful acts using ICTs STATE SOVEREIGNTY for: state sovereignty applied to State's ICT activities & ICT infrastructure within their territory

ID	Document	Document Groups	Quotation Content	Codes
175:3	2013 - U.S.-Russian+Cooperation	2013	To prevent crises, the United States and Russia also recognize the need for secure and reliable lines of communication to make formal inquiries about cybersecurity incidents of national concern. In this spirit, we have decided to use the longstanding Nuclear Risk Reduction Center (NRRC) links established in 1987 between the United States and the former Soviet Union to build confidence between our two nations through information exchange, employing their around-the-clock staffing at the Department of State in Washington, D.C., and the Ministry of Defense in Moscow. As part of the expanded NRRC role in bilateral and multilateral security and confidence building arrangements, this new use 3/2/2018 FACT SHEET: U.S.-Russian Cooperation on Information and Communications Technology Security | whitehouse.gov https://obamawhitehouse.archives.gov/the-press-office/2013/06/17/fact-sheet-us-russian-cooperation-information-and-communications-technol 3/3 of the system allows us to quickly and reliably make inquiries of one another's competent authorities to reduce the possibility of misperception and escalation from ICT security incidents.	STAKEHOLDER COOPERATION CBM: states should participate and cooperate in multilateral forums STATE RESPONSIBILITY for: adhering to rules and regulations agreed upon by previously enacted international law/mandates/treaties
176:1	2012 - Chairs.Summary.IGF.2012	2012	While the session was overwhelmingly optimistic, there was an underlying message delivered regarding the supreme importance of securing a safe and secure Internet for young people and the generations to com	NORM for: promote an open, secure, stable, accessible, and peaceful cyber space / ICT environment
176:2	2012 - Chairs.Summary.IGF.2012	2012	principles of human rights.	HUMAN RIGHTS for: respecting human rights and fundamental freedoms; applying them to cyber space / ICT use, etc.
176:3	2012 - Chairs.Summary.IGF.2012	2012	These existing laws together with education and outreach to new consumers of online content, especially those using mobile devices, was said to be crucial in assuring privacy and safety. It was agreed that certain new cyber- threats such as identity theft needed special attention and innovative regulatory and legal policy solutions.	CYBER ATTACK for: preventing ICT-enabled theft of intellectual property (this includes trade secrets and other confidential business information) EDUCATE AND STRENGTHEN THE GENERAL PUBLIC for: providing users/customers/the general public with information and tools that will enable them to understand current and future threats, as well as protect against them STAKEHOLDER COOPERATION for: working with partners / sharing responsibility in identifying threats and keeping shared network's safe STATE RESPONSIBILITY for: adhering to rules and regulations agreed upon by previously enacted international law/mandates/treaties
176:4	2012 - Chairs.Summary.IGF.2012	2012	Their discussions had focused on what was required to get women to have access; on education and skills building to empower women to get online; the challenges of cyber-crime and violence directed at women and how these can force women to stay offline, and, empowering women to overcome these challenges.	DIGITAL EQUALITY CBM: work towards digital equality and inclusion (i.e., for women and traditionally marginalised groups) - this includes cooperation between the private sector, civil society, and national governments (as well as multilateral banks, and international entities such as the United Nations) DIGITAL EQUALITY for: closing the gender digital divide (focusing on women and girls, but also those a part of gender subgroups such as the LGBTQI+ communiy) HUMAN RIGHTS for: addressing online gender-abuse/violence through a human rights framework STAKEHOLDER COOPERATION for: coordinate/cooperate in combatting cybercrime
176:5	2012 - Chairs.Summary.IGF.2012	2012	Policy issues regarding both domestic and trans-border cyber-crime were also discussed in depth during the session. Subject experts emphasized the increasing complexities of such attacks, noting also that the technology enabling this behavior is only going to become more sophisticated and harder to combat. Who should bear the responsibility for preventing these attacks? Arguments can be made that this responsibility should fall on government policy makers, national militaries, Internet intermediaries or individual users themselves. It was stressed that it was not one actor but rather the multi-stakeholder community that should be addressing this dangerous and burgeoning threat	STATE SOVEREIGNTY disagreement: finding States at fault for internationally recognized wrongful ICT acts committed by on state territory
176:6	2012 - Chairs.Summary.IGF.2012	2012	rather the multi-stakeholder community that should be addressing this dangerous and burgeoning threat	STAKEHOLDER COOPERATION for: coordinate/cooperate in preserving multistakeholder internet governance

ID	Document	Document Groups	Quotation Content	Codes
176:7	2012 - Chairs.Summary.IGF.2012	2012	Azerbaijan is in the midst of a significant economic transformation and ICTs and Internet connectivity are the tools that are aiding its development into a knowledge- based and innovative society	ACCESS CBM: creating a free flow of and acccess to the internet is essential for the digital economy, and beneficial to development CONFIDENCE BUILDING CBM: recognize importance of ICTs as the key driver of governance, economy, commerce, trade, and social well-being NORM for: supporting a free and secure internet / cyber space that supports economic growth and innovation
176:8	2012 - Chairs.Summary.IGF.2012	2012	The youth of Azerbaijan are benefitting in particularly from Internet technologies and significant government spending on initiatives supporting youth and ICT. Integrating ICTs into education at all levels and enabling young people to become innovative entrepreneurs is a top priority of the government.	EDUCATION for: include cybersecurity courses in school curricula (i.e., primary school, degree courses in undergrad, professional education, and trainings EDUCATION for: increased eduation, [digital] literacy, and awareness regarding digital rights and ways to exercise/protect them
177:1	2012 - Eleventh Meeting of the Russian Federation, India and China	2012	The Foreign Ministers of the Russian Federation, the Republic of India and the People's Republic of China held their 11th meeting in Moscow on 13 April 2012.	INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information
177:2	2012 - Eleventh Meeting of the Russian Federation, India and China	2012	The Ministers reiterated the importance attached by Russia, India and China to their constructive cooperation in the trilateral format. They stressed that this cooperation was not directed against any other country, was conducive to the promotion of regional peace, security and stability and served to beneft their peoples.	STAKEHOLDER COOPERATION CBM: states should participate and cooperate in multilateral forums
177:3	2012 - Eleventh Meeting of the Russian Federation, India and China	2012	The Ministers afrmed that Russia, India and China intended to closely cooperate in addressing these challenges, including by consulting among themselves in the framework of the UN and relevant multilateral fora.	UNITED NATIONS CBM: the United Nations (UN) may serve as an international body for decision-making, framework creation/implementation, and when developing and adopting universally agreed upon ICT norms/rules/principles (in order to ensure peace and responsible behavior/ICT use)
178:1	2011 - IGF.2011. Chair's Summary copy	2011	The Secretary General of the International Telecommunications Union, Hamadoun Touré, spoke of the diverse activities of the Union. He spoke of the work of the ITU 3 and its member states in cyber-security, child online protection and climate change. The Secretary General also shared with delegates some of the insights that had emerged in the high level dialogue that the ITU had organised with the Government of Kenya prior to the IGF.	INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information STAKEHOLDER COOPERATION CBM: states should participate and cooperate in multilateral forums
178:2	2011 - IGF.2011. Chair's Summary copy	2011	he concept of safety expanded the debate and the need for policy development beyond the call for cyber-crime treaties and into a multi-stakeholder dialogue where all can benefit from the synergies, whether the issue was one of protection of children and the vulnerable online to ensuring the security and stability of the Internet itself.	DIGITAL EQUALITY for: the protection of digital rights should be embedded in an inclusive approach (i.e., also considers the needs/rights of vulnerable groups such as children, women, gender minorities, people w/ disabilities, etc.) STAKEHOLDER COOPERATION for: coordinate/cooperate in preserving multistakeholder internet governance
178:3	2011 - IGF.2011. Chair's Summary copy	2011	This session discussed the cross-border Internet governance issues that are encountered at the intersection of security, openness and privacy. Further, the issue of human rights was prominent throughout the discussion. Many of the examples debated in the session linked to events of the past year, such as actions taken by a range of Internet actors in relation to whistleblowers sites, the “seizure” of domain names, proposals for blocking of websites and filtering of networks, the role that cyber security operations centers and law enforcement can play in protecting the Internet and its users from cyber-attacks and cybercrime, and the impact of actions taken to cut access to the Internet for individuals, groups or entire countries, as was the case during the ‘Arab Spring’.	ACCESS for: support the free flow of information while respecting applicable legal frameworks for privacy and data protection CONFIDENCE BUILDING for: ensuring the free flow of data while also protecting the integrity of that data and the privacy of individual users HUMAN RIGHTS for: respecting human rights and fundamental freedoms; applying them to cyber space / ICT use, etc. NORM for: promote an open, secure, stable, accessible, and peaceful cyber space / ICT environment STATE RESPONSIBILITY for: enacting cybersecurity measures that will protect people (privacy, and physical safety, etc) and inform users (transparency)
178:4	2011 - IGF.2011. Chair's Summary copy	2011	There was a lively debate about where the responsibility lies when it comes to cyber- security. Individual users, families, Internet service providers, independent law makers and regulators, State governments and global policy making institutions were all said to hold such responsibility. Ongoing capacity building and education of users on all of the issues is absolutely necessary	CAPACITY BUILDING CBM: encourage further work in capacity-building STATE RESPONSIBILITY CBM: repository of national laws/policies for data protection and ICT infrastructure STATE RESPONSIBILITY for: enacting cybersecurity measures that will protect people (privacy, and physical safety, etc) and inform users (transparency)

ID	Document	Document Groups	Quotation Content	Codes
178:5	2011 - IGF.2011. Chair's Summary copy	2011	The well-established policy frameworks in the ICT sector that support investment, innovation, new services and dramatic increases in access with lower prices and higher qualities need to be replicated across the whole Internet	ACCESS CBM: access to the internet is an important enabler of development./growth/innovation NORM for: supporting a free and secure internet / cyber space that supports economic growth and innovation
179:1	2011 - Aus-US SR46_cybersecurity_v2	2011	At the 15 September 2011 AUSMIN talks in San Francisco, Australian and US offcials took advantage of the 60th anniversary of the signing of the ANZUS Treaty to announce the alliance would now extend into cyberspace. It was the frst time, outside of NATO, that two allies had formalised their joint cooperation in cyberspace.	INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information STAKEHOLDER COOPERATION CBM: form bilateral and multilateral cooperation initiatives to build on established partnerships/relationships
179:2	2011 - Aus-US SR46_cybersecurity_v2	2011	Although the US seeks to promote an internet freedom agenda, capacity building and security in economic transactions, Russia and China defne cybersecurity as the control of content, communication and interaction in cyberspace so that they don't undermine domestic governance and political stability.	CAPACITY BUILDING CBM: encourage further work in capacity-building STATE SOVEREIGNTY for: state sovereignty applied to State's ICT activities & ICT infrastructure within their territory
179:3	2011 - Aus-US SR46_cybersecurity_v2	2011	both in economic forums (the Council of Europe and the Organisation for Economic Co-operation and Development) and in military security organisations (such as NATO). The report also discussed openness and innovation in internet governance; building capacity, security and prosperity on the international level; and international freedom.	STAKEHOLDER COOPERATION CBM: states should participate and cooperate in multilateral forums
180:1	2011 - Russian+Convention+on+International+Information+Security	2011	and that it is necessary to stimulate, form, develop, and 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", noting the necessity of activating efforts to overcome the "digital divide" by increasing the ease of supply of information and communication technology to developing countries, and increasing their potential in relation to cutting-edge practices and professional training in the sphere 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",	STATE RESPONSIBILITY for: adhering to rules and regulations agreed upon by previously enacted international law/mandates/treaties UNITED NATIONS CBM: the United Nations (UN) may serve as an international body for decision-making, framework creation/implementation, and when developing and adopting universally agreed upon ICT norms/rules/principles (in order to ensure peace and responsible behavior/ICT use)
180:2	2011 - Russian+Convention+on+International+Information+Security	2011	15) States Parties should support and stimulate scientifc and technical developments connected with the exploration of the information space, as well as educational activity, aimed at forming a global culture of cybersecurity; 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;	CONFIDENCE BUILDING CBM: further investments in ICT research and development HUMAN RIGHTS for: respecting human rights and fundamental freedoms; applying them to cyber space / ICT use, etc. INFORMATION EXCHANGE CBM: encouraging exchanges between research and academic institutions NORM for: promote an open, secure, stable, accessible, and peaceful cyber space / ICT environment
180:3	2011 - Russian+Convention+on+International+Information+Security	2011	20) States Parties stimulate the partnership between business and civil society in the information space; 21) States Parties acknowledge their responsibility to ensure that citizens, public and state bodies, other States, and the global community are informed about new threats to the information space and about known methods of increasing the level of their security.	EDUCATION for: increased eduation, [digital] literacy, and awareness regarding digital rights and ways to exercise/protect them STAKEHOLDER COOPERATION for: work with states and/or the private sector/civil society (international and/or domestic) to further cooperate on topics such as law enforcement, prosecution, investment, e-commerce, intellectual property rights, etc.
180:4	2011 - Russian+Convention+on+International+Information+Security	2011	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 confict, 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	STATE SOVEREIGNTY for: state sovereignty applied to State's ICT activities & ICT infrastructure within their territory
180:5	2011 - Russian+Convention+on+International+Information+Security	2011	5) each State Party has the right to make sovereign norms and govern its information space according to its national laws. Its sovereignty and laws apply to the information infrastructure located in the territory of the State Party or otherwise falling under its jurisdiction. The States Parties must strive to harmonize national legislation, the differences whereof must not create barriers on the road to a reliable and secure information space;	DOMESTIC LAW for: applicability of domestic law to cyber space / ICT usage INTERNATIONAL LAW for: applicability of international law to cyberspace

ID	Document	Document Groups	Quotation Content	Codes
181:1	2010 - IGF 2010.Chairman's.Summary	2010	With close to 2000 badges issued and 1461 participants, attendance at the Vilnius meeting was similar to the 2009 meeting in Sharm El Sheikh. Parallel to the main sessions, 113 workshops, best practice forums, dynamic coalition meetings and open forums were scheduled around the broad themes of the main sessions and the overall mandate of the IGF.	INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information STAKEHOLDER COOPERATION CBM: states should participate and cooperate in multilateral forums STATE RESPONSIBILITY for: dialogue amongst nations by an international body
181:2	2010 - IGF 2010.Chairman's.Summary	2010	The session also addressed issues of international cooperation and collaboration, and considered human rights norms and conventions. The Budapest Convention was mentioned as one of the tools that addressed cybercrime standards and norms. It had the force of law and could potentially be applied worldwide and had been drafted with the participation of non-European countries.	CONFIDENCE BUILDING CBM: adopt legislative basis for combatting cybercrime (i.e., the Budapest Convention)
181:3	2010 - IGF 2010.Chairman's.Summary	2010	Needs to be understood from the perspective of a sustainable development that meets three needs: social equity, preserving the environment, and economic efficiency; • Is governance that adequately and proportionally represents developing countries in its mechanisms and processes; • Must enable innovation in developing countries; • Advances the development of the Internet in developing and transitional countries and promotes Internet enabled development; • Takes a global view and is governance for both the developing and developed worlds.	ACCESS CBM: access to the internet is an important enabler of development./growth/innovation ASSIST for: adopting appropriate policies and measures so that developing countries benefit from the advantages of technological progress (and do not suffer from lack of early adoption) ASSISTANCE CBM: provide assistance and training to developing countries to improve cybsecurity and ICT use STAKEHOLDER COOPERATION for: coordinate/cooperate in preserving multistakeholder internet governance
181:4	2010 - IGF 2010.Chairman's.Summary	2010	Openness and privacy were examined through three thematic lenses: • Issues related to social media. • The nature and characteristics of Internet networks, technologies, and standards. • International cooperation and collaboration on security, privacy and openness.	ACCESS for: support the free flow of information while respecting applicable legal frameworks for privacy and data protection CONFIDENCE BUILDING for: ensuring the free flow of data while also protecting the integrity of that data and the privacy of individual users NORM for: promote an open, secure, stable, accessible, and peaceful cyber space / ICT environment STATE RESPONSIBILITY for: enacting cybersecurity measures that will protect people (privacy, and physical safety, etc) and inform users (transparency)
181:5	2010 - IGF 2010.Chairman's.Summary	2010	From a human rights perspective, the right to privacy was a fundamental permanent right and security was a necessity for exercising all rights. So what was needed was not to balance security against privacy but to work out how to enhance both simultaneously and not allow one to erode the other.	HUMAN RIGHTS for: respecting human rights and fundamental freedoms; applying them to cyber space / ICT use, etc.
181:6	2010 - IGF 2010.Chairman's.Summary	2010	• Status of IPv6 availability around the world; examples and cases; • The internationalization of critical Internet resources management and enhanced cooperation; • The importance of new TLDs and IDNs for development; • Maintaining Internet services in situations of disaster and crisis	CRITICAL INFRASTRUCTURE for: protecting critical infrastructures
182:1	2010 - Australia-United States Ministerial Consultations	2010	Minister for Foreign Affairs Kevin Rudd, Minister for Defence Stephen Smith, Secretary of State Hillary Rodham Clinton and Secretary of Defense Robert Gates met in Melbourne on 8 November 2010 for the annual Australia–US Ministerial Consultations (AUSMIN).	INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information
182:2	2010 - Australia-United States Ministerial Consultations	2010	Australia and the United States reaffirmed that strengthened architecture in the Asia–Pacific region is fundamental to security and economic prosperity. Both countries welcomed the expansion of the East Asia Summit (EAS), to include the participation of the United States from 2011. The United States welcomed Australia's leading role as an advocate for strengthened regional institutions, and for a more significant role for the EA	CAPACITY BUILDING CBM: develop regional approaches to capacity-building STAKEHOLDER COOPERATION CBM: form bilateral and multilateral cooperation initiatives to build on established partnerships/relationships STAKEHOLDER COOPERATION CBM: states should participate and cooperate in multilateral forums STAKEHOLDER COOPERATION for: support other international and/or regional cooperative partnerships
182:3	2010 - Australia-United States Ministerial Consultations	2010	Recognising the increasing sophistication of threats against both countries in cyberspace, Australia and the United States intend to promote a secure, resilient and trusted cyberspace that assures safe and secure access for all nations. Both countries recognised the benefits to be derived from enhanced collaboration when operating and defending mutual national interests in cyberspace, including shared defence and economic interests. Both countries committed to work together to advance the development of shared international norms for cyberspace	CRITICAL INFRASTRUCTURE for: promoting resilience (as related to ICTs,cybersecurity, and related critical infrastructure NORM for: promote an open, secure, stable, accessible, and peaceful cyber space / ICT environment

ID	Document	Document Groups	Quotation Content	Codes
183:1	2009 - IGF Chairman Summary	2009	With more than 1800 participants from 112 countries the Sharm meeting had the biggest attendance so far. 96 governments were represented. 122 media representatives were accredited.	INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information STAKEHOLDER COOPERATION CBM: states should participate and cooperate in multilateral forums
183:2	2009 - IGF Chairman Summary	2009	and the global community should ensure that barriers to participation by developing countries should be removed.	ASSIST for: adopting appropriate policies and measures so that developing countries benefit from the advantages of technological progress (and do not suffer from lack of early adoption) ASSISTANCE CBM: provide assistance and training to developing countries to improve cybsecurity and ICT use
183:3	2009 - IGF Chairman Summary	2009	The Prime Minister saw in the continuation of the IGF a real priority. The IGF had provided a valuable space for continuous education on the prospects of the Internet and the global cyberspace and it was a precious learning tool for the young generations	EDUCATION CBM: skills development, particularly for younger individuals (both internal and external, international and/or domestic)
183:4	2009 - IGF Chairman Summary	2009	It was recommended that in terms of achieving the appropriate balance between security, openness and privacy, people should use their buying power to convince vendors to improve the security of their products, and should fund research more broadly. The Council of Europe's Convention on Cybercrime was also mentioned as part of the solution on how to deal with security.	STAKEHOLDER COOPERATION for: support other international and/or regional cooperative partnerships
183:5	2009 - IGF Chairman Summary	2009	global forum of peace, using the Internet.	NORM for: promote an open, secure, stable, accessible, and peaceful cyber space / ICT environment
183:6	2009 - IGF Chairman Summary	2009	In the final part of the Honourary Session, Ms. Mubarak witnessed the signing four partnership agreements on behalf of the Cyber Peace Initiative with key organizations and multinational corporations and presented three certificates of recognition to young people and organizations that excelled in serving the young generations through ICTs.	NORMS CBM: national declarations of adherence to the normative framework of responsible State behavior could build trust and confidence between states
183:7	2009 - IGF Chairman Summary	2009	the Arab and East Africa region described the creation of CERTs/CSIRTs at the national and regional levels as priorities that should be implemented.	EMERGENCY RESPONSE CBM: assist in strengthening cooperation amongst national computer ER teams etc. EMERGENCY RESPONSE CBM: each state/regional partnership should establish and/or strengthen a national computer emergency response team (CERT) / cybersecurity incident response team
183:8	2009 - IGF Chairman Summary	2009	Many specific examples were given of work that was being done that clearly responded directly to the WSIS principles. One example was the multistakeholder work that had been done by the Council of Europe, the Association for Progressive Communications and the United Nations Economic Commission for Europe on the development of a trilateral initiative to launch a code of good practice on information, participation, and transparency in Internet governance	CONFIDENCE BUILDING CBM: voluntary transparency INFORMATION EXCHANGE for: sharing of good/best practices in relation to ICTs and cybersecurity UNITED NATIONS CBM: the United Nations (UN) may serve as an international body for decision-making, framework creation/implementation, and when developing and adopting universally agreed upon ICT norms/rules/principles (in order to ensure peace and responsible behavior/ICT use)
183:9	2009 - IGF Chairman Summary	2009	promote greater participation by all stakeholders to inform and provide their perspectives.	STAKEHOLDER COOPERATION for: encourage participation of other stakeholders such as the private sector, academia, and civil society orgs (as appropriate) for CBM and/or norm creation and implementation STAKEHOLDER COOPERATION for: stakeholders working together on achieving an appropriate balance between the interests of citizens/entities to secure their data, and the needs of law enforcement agencies (while not undermining the fundamentals of technology)
183:10	2009 - IGF Chairman Summary	2009	ensuring the security and stability of the Internet.	CYBER STABILITY for: maintaining a secure, safe, and trustable ICT environment
183:12	2009 - IGF Chairman Summary	2009	asked for more openness and multistakeholder participation in intergovernmental organizations.	STAKEHOLDER COOPERATION for: coordinate/cooperate in preserving multistakeholder internet governance
183:13	2009 - IGF Chairman Summary	2009	This meant there would need to be a human rights perspective beyond technological development and commercial developments. The interaction of all these elements was from a human rights policy and perspective, which would guarantee that the focus would be on human beings and their benefit.	HUMAN RIGHTS for: respecting human rights and fundamental freedoms; applying them to cyber space / ICT use, etc.
183:14	2009 - IGF Chairman Summary	2009	Enhanced cooperation generally and the internationalization of critical Internet resource managemen	CRITICAL INFRASTRUCTURE for: protecting critical infrastructures
183:15	2009 - IGF Chairman Summary	2009	The panellist finally emphasized the importance of foreign companies in complying with local laws	DOMESTIC LAW for: applicability of domestic law to cyber space / ICT usage

ID	Document	Document Groups	Quotation Content	Codes
183:16	2009 - IGF Chairman Summary	2009	The terms of use of many social media and services were described as being complex, and users were not always clear of their rights and responsibilities, therefore literacy training was proposed as being necessary.	EDUCATION for: increased eduation, [digital] literacy, and awareness regarding digital rights and ways to exercise/protect them
184:1	2008 - IGF Chairman's Summary.10.12.2	2008	In order to promote education and other services and access to the Internet, the Government of India had embarked on a national programme to make the Internet available to the citizens through common service centres.	ACCESS CBM: access to the internet is an important enabler of development./growth/innovation
184:2	2008 - IGF Chairman's Summary.10.12.2	2008	Without appropriate information, people could not adequately exercise their rights as citizens.	EDUCATION for: increased eduation, [digital] literacy, and awareness regarding digital rights and ways to exercise/protect them
184:3	2008 - IGF Chairman's Summary.10.12.2	2008	The IGF was appreciated for its open multistakeholder model, with examples of new national and regional IGF initiatives illustrating the spread of the multistakeholder ideal and its value in policy discussion	INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information STAKEHOLDER COOPERATION for: coordinate/cooperate in preserving multistakeholder internet governance
184:4	2008 - IGF Chairman's Summary.10.12.2	2008	While in the off-line world the perpetrator of a crime could be traced to the locality where the crime was committed, this was not the case anymore in the on-line world. Law enforcement therefore was confronted with problems of jurisdiction and geographical boundaries	STAKEHOLDER COOPERATION for: coordinate/cooperate in combatting cybercrime
184:5	2008 - IGF Chairman's Summary.10.12.2	2008	It was noted that most off-line crimes had now also moved on-line. There were also new forms of crime that were specific to the Internet, such as hacking or phishing. In addition, there were also attacks on a country's critical infrastructure, such as distributed denial of service attacks (DDOS).	CRITICAL INFRASTRUCTURE for: promoting resilience (as related to ICTs,cybersecurity, and related critical infrastructure CRITICAL INFRASTRUCTURE for: protecting critical infrastructures
184:6	2008 - IGF Chairman's Summary.10.12.2	2008	The session started off with a mention of the conflict in the sense of national security versus security for privacy, and the right to information and a mention of how increasing the level of user security and privacy, confidence and trust could be engendered for use of Internet and facilitated free expression of opinion. The Chair spoke of how the Internet was global, but privacy could be local, regional or national in context. As the Internet had become a way of life, there were societal issues which needed to be addressed. In the Indian context, it was explained that nine million subscribers were being added every month. Governance was considered to become a relevant point in these circumstances.	ACCESS for: support the free flow of information while respecting applicable legal frameworks for privacy and data protection CONFIDENCE BUILDING for: ensuring the free flow of data while also protecting the integrity of that data and the privacy of individual users STATE RESPONSIBILITY for: enacting cybersecurity measures that will protect people (privacy, and physical safety, etc) and inform users (transparency)
184:7	2008 - IGF Chairman's Summary.10.12.2	2008	Universal Declaration of Human Rights (UDHR) with regard to the free flow of information and its importance. • The Tunis Agenda was a high watermark for the commitment to free flow of information, both in paragraphs 4 and in 42. • The OECD ministerial contained many important statements there on the free flow of information. • The International Telecommunications Union at the World Telecommunication Standardization Assembly, offered in Rresolution 69 an strong statement about the free flow of information in which Member States were invited to refrain from taking any unilateral or discriminatory actions that could impede another Member from accessing public Internet sites. • The Global Network Initiative which brough together a number of NGOs and companies with the aim to address the issues of protecting freedom of expression and privacy for users.	STATE RESPONSIBILITY for: adhering to rules and regulations agreed upon by previously enacted international law/mandates/treaties
184:8	2008 - IGF Chairman's Summary.10.12.2	2008	The moderator brought up the confluence of freedom of sexual expression, as content on the Internet, with the discussion of protection of children.	DIGITAL EQUALITY for: the protection of digital rights should be embedded in an inclusive approach (i.e., also considers the needs/rights of vulnerable groups such as children, women, gender minorities, people w/ disabilities, etc.)
184:9	2008 - IGF Chairman's Summary.10.12.2	2008	The representative of the United States of America said the Internet in its uses had begun to involve governments, the private sector and civil society in new forms of enhanced cooperation on an unprecedented scale.	STAKEHOLDER COOPERATION for: encourage participation of other stakeholders such as the private sector, academia, and civil society orgs (as appropriate) for CBM and/or norm creation and implementation
184:10	2008 - IGF Chairman's Summary.10.12.2	2008	One panellist explained how the whole debate about privacy, openness, and security could be shown in the dimension of women's human rights. The discussion focused on the specific issue of sexual rights defined in the Cairo Program of Action, as a state of physical, emotional, mental, and social well-being related to sexuality. This definition was not merely related to the absence of disease, dysfunction, or infirmity, but it also required a positive approach to sexuality and sexual relationships as well as the possibility of having safe sexual experiences, free from coercion, discrimination, and violence.	DIGITAL EQUALITY CBM: work towards digital equality and inclusion (i.e., for women and traditionally marginalised groups) - this includes cooperation between the private sector, civil society, and national governments (as well as multilateral banks, and international entities such as the United Nations) DIGITAL EQUALITY for: closing the gender digital divide (focusing on women and girls, but also those a part of gender subgroups such as the LGBTQI+ communiy)

ID	Document	Document Groups	Quotation Content	Codes
184:11	2008 - IGF Chairman's Summary.10.12.2	2008	The numerous human rights where discussed as having a direct bearing on sexual rights and sexual health. These included the right to liberty and security of the person, the right to be free from torture and inhuman and degrading treatment, the right to private and family life, the right to nondiscrimination, and, specific to this session, the right to information and education	HUMAN RIGHTS for: addressing online gender-abuse/violence through a human rights framework HUMAN RIGHTS for: respecting human rights and fundamental freedoms; applying them to cyber space / ICT use, etc.
184:12	2008 - IGF Chairman's Summary.10.12.2	2008	A new treaty would promote solidarity and cooperation between States and underline the public value of the Internet beyond commercial interests, in full respect of international law, including human rights law. Signing up to a new multilateral treaty which ensured the functioning of the Internet would be of fundamental importance to keep the Internet open and free in the interest of future generations	INTERNATIONAL LAW for: applicability of international law to cyberspace STAKEHOLDER COOPERATION CBM: states should participate and cooperate in multilateral forums
184:13	2008 - IGF Chairman's Summary.10.12.2	2008	Reports were received from a number of regional and national IGF initiatives, other related events, and other meetings that took place during the Hyderabad IGF. A European Dialogue on Internet Governance (EuroDIG) was held in Strasbourg on 20-21 October 2008. The meeting focused on European perspectives and at the center of discussions was the notion of fostering security, privacy and openness. The meeting wanted to produce some agreed outcome but without negotiating texts, and developed a format with 'Messages from Strasbourg', with reports produced by editors on different topics discussed at the meeting.	STAKEHOLDER COOPERATION for: support other international and/or regional cooperative partnerships
184:14	2008 - IGF Chairman's Summary.10.12.2	2008	two best practice forums	INFORMATION EXCHANGE for: sharing of good/best practices in relation to ICTs and cybersecurity
185:1	2008 - Shanghai+Cooperation+Org Agreement	2008	la rEL z -15- — g.cc 7 RcA 5 =clg co o tai tomeezam e,,` 5a0c2 ' E 005- _,V4 0 Nl di [C 0 21 2(11t2A&g cn goa'Ds.“4. F-7 4 @E-g- sS lAi R 7).3 8 .5- S'E cilg mm—an m C-1532:A=3 S. 0 Al agE0Eg Fee 92-c Ts ca 45 e to [DD z 8pc a- --0g S m n 2- 0 5 0 c ▪ x, -r.4) ta • s - 6._ 3' co a	INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information STAKEHOLDER COOPERATION CBM: states should participate and cooperate in multilateral forums
185:2	2008 - Shanghai+Cooperation+Org Agreement	2008	E-0.cL =0z.-ci) ..q,#-'010- -..4.-____;,,,S-.‹. -rf.5-g..=- 7. S0', 6a,tg,F5 6 -mc,4m -.Pag:6g2FrlAR ". c ri 0 - a' 9-, ' co 3 x-cp 0 _, c --- DEC ij 6 0 r::i 5c,-,,M al ,n E,. r_ m 7 13 -, a g. cn a S N c 5- 4 cri - M- CnCOU ' DIM — 150 g wean - ,..11 -.- 0 • 0- 4n c? —a 0 '6 el ra cT iagra"ei; 03, m =: = eD 5 F S'5' ,=-'050 . 1k 5 3'433 ,.. . ,, F-. at di rA a" 0 di R cii - m Fic Si ai 9 j 0 — o 94 .2w co —, _, - rn mcrm6 m a m 60-- 0 n Ri cn = .5 ._ 6 -;:- o .07-1c 0 ,,,,. N :5 0 ?„ _i C- 5 C. = F ,-. 0 = . 7 Cr 01 = LO 51 t ,' , 17 7-co 0 0 CD = , - -0 5., c_,,, c Evo. to 7- F, ... = - .. 0 , s•Z o_. ..20g. n o 'cl ,.. mZ -0,-.:.sz- a. z — Tiff, CD ... ,-,,a)=4,. z=.c.a o -0 a 5'a S su c75- _„„ 0 7.1 g 93 et = oo Q * a O. ...i; 411 me r= = — 0 A cm 7 a' • - 0-a..... 0 , ..,:.. 4) 4: 5' „ 1 41 C,.Lt6 .., ,-■ LT.,' 5 z 2- co E 82' „; -:. = ,•D 7 c 9' 5 c5 5/1 — = c2 a eD 5 8 g 0	UNITED NATIONS CBM: the United Nations (UN) may serve as an international body for decision-making, framework creation/implementation, and when developing and adopting universally agreed upon ICT norms/rules/principles (in order to ensure peace and responsible behavior/ICT use)

ID	Document	Document Groups	Quotation Content	Codes
185:3	2008 - Shanghai+Cooperation+Org Agreement	2008	=-- 2 tl'i eD ' = 2 0 c 5 o _ ,-,-. ,,-,1- .0. - -. .,, -1K > cL 0 7', 2 1r, 5 t: _, a. a cr JD (0 = co R -4 .-0 -Z,- .m ell .o. F, • 3 c.-D IS c :--.-=`.. 0 > 4 05 - za = - - c e5 47 Z ,=4. cz a) =- -s.) ,ep-k 3_ - Li 0 -- ----- - ....._..0__..=-74- -- 0-- ---- . in. 0 7'. 03 .-%--- ..-:---.--. z m_ - 7 q. .,...-.9 c-). --k- 0,:' ca---...-- c • ,..--.... .t.. 0 c ,--L- .-..m-'---irs- - - ...• ,. - -,....'a ,7,•' .-;_.. ;647 a) ca co co -'-, ----0 .--- _. c.,- ---- s s, (4,.1, it- 0 0 nc c 0 . r; '...) a. D - E- 3 2 ,,, -' al, E. (D CD L5 en 3al m 7 CO ,.... ' - -cl 7 '(8 >--1 cz 0 cl) 0 c- 5 y" -1 ❑ E 75' '" 4 a' ----P. a ,2 7-,- - 6 , i cn -q2- ❑ f, i 5 1 g 7.. g 21 t- 2 _,-. 1 . '1] ❑' a' '" ':;* ivi 2 d •a . Er > g 2 g "0 0, ❑ Sci- 9 g 2) m❑ 6 5 _-C- e7 a, = .,- = 0 6 , = - , = ,2 CI Fi :2: 5' us a " 8m06.o.s.co - .1. l'- , 05 1 -. 1 @,-, ,, 7 =' 0" = •, 5 - cs -%. 0 7 5 - a; ea r 0,-- ,c?, ss. E. „„. 0 0 001 - To „„ . Ei ',,--... r:g Q Lc w lni •--1' 5 '7 ° 8 ='" 5 -- -C 5- F - •c1 -, n a.. 0 La 0 a, 3 0.0 . 42 tD ,.,. a; > (1,- 8 D ..••• (Ty ...., OS 0 2 ,-* 3 8 d on 54. 5 '5' C 8 Eli 5* = c =4 c - o-- es .4. .7..'" = m C co Ch en (.5 e.-. CD = ,. --• 17i c ,-co---,0 ra. .,: - - co-`7r 7, °0• c" al a - 8 C3 n 3 2DI 13, F2.4 ,,, CD - Ei,-.: 0 0 - - 4 3 2. 9q0 8 c;50a . ca Ft . 6 C.() 5 . - CA 0 os 7.1 = a, -- =_ 5 5 e-,0 ;' co -. 5 ila ri) - 5 5 a FO' C L. 2 . 0 3 it, 5 ' ' 0 'V laa - NI © 8' 2 0 ..Z 3 - c . 0 5_. -., I. CD is. ,F z.o# ifi c o 2, 1 _.. .-, ,,, co 5. .... 5 wars g - E 3.elcg , 5 :a Qco - cn c'J 0 CO C .", 2 03 R 00 5- C4 A -, =, , ,, - n P'. z= - . " ... Id'- c90 m 0 .,., - '" 5 P. --- co c - ° Ck sv "5 P.- 2. ,,, c 0. IT z CD DI CD fa {D- 5 0 • s..,T NI ig ,- co, •. 3 '" 5 5 - {-13' ❑ n AD S. En - = c i- ,..., - 5' a = - .7.s. n115 5 .-=) z . n ...., --, a F- 0 C.... S3 3, 5. - a 0 _.co0ra = , c 0 5 R• 1:1 0 ,.. - = a; 4.: w a: cr; c2,, 2 -0 c n . o . F, Z 13 s. -, c11 ' -I cT: , c=„, a 5:4. LC - 7 .2Fri, m: a c . 0 15 8 - - 1 . -cm (I - o d -; 0 A C C - = 0) 0 W :!. n a CD to 5 ,.... Fli "C-5 . n E. = s...) as .7...; o 0) --- on _,. 0 -ti E- 5 - ,+ =. = .'''" Da ' ff- to Qc c 4 c la &I p. a. 5• ra - ' w .0 ❑ el 8 a ' 9 , 8' 5- n. r iz f`-' 0- 2 T*. 3@ 15. m - 55- 6 6T1 co 5 - n0,... -" .T.- .. --, -. c .=-° o - , .-- 0 a... -, a(a) d 0 5 g c:5• =• a - P-'- C5. m'. ti = e. 0 tu (5-g 0 al - -- m 0 0m - • 0 a _ .-% ... -ci ..4 -. 0 5' -1:1 -0 5. OD 5. 59, , c cp ...., 7 = co C2e CID 3 ,cc ci e •r1 3. 0. - a to et o c ca ❑ ZE 7 -- as-) c,., c. Qs -=0 aCD 0 ".' cr 0 CD 0 0 35t4 -' . a c- CQ g2:. . z -;.„ 5. 5 ,.., 0 IA as .< -. . ... ..fr: 0 . 0 50 3 ,c = 0,1 .,.. um .,. a - a 0 ,.... ...4 cff m - 5 F [n • 7 co - .. (1 , co 0, CL Zi co . (0 M Q- .6	CYBER ATTACKS for: strengthen tools and resources needed to prepare, deter, defend, and respond to unlawful use of ICTs, cyber attacks / acts of cyber crime and/or terrorism
185:4	2008 - Shanghai+Cooperation+Org Agreement	2008	, 8'. ❑ '=-- 2 tl'i eD ' = 2 0 c 5 o _ ,-,-. ,,-,1- .0. - -. .,, -1K > cL 0 7', 2 1r, 5 t: _, a. a cr JD (0 = co R - 4 .-0 -Z,- .m ell .o. F, • 3 c.-D IS c :--.-=`.. 0 > 4 05 - za = - - c e5 47 Z ,=4. cz a) =- -s.) ,ep-k 3_ - Li 0 -- ----- - ....._..0__..=-74- -- 0-- ---- . in. 0 7'. 03 .-%--- ..-:---.--. z m_ - 7 q. .,...-.9 c-). --k- 0,:' ca---...-- c • ,..--.... .t.. 0 c ,--L- .-..m-'---irs- - - ...• ,. - -,....'a ,7,•' .-;_.. ;647 a) ca co co -'-, ----0 .--- _. c.,- ---- s s, (4,.1, it- 0 0 nc c 0 . r; '...) a. D - E- 3 2 ,,, -' al, E. (D CD L5 en 3al m 7 CO ,.... ' - -cl 7 '(8 >--1 cz 0 cl) 0 c- 5 y" -1 ❑ E 75' '" 4 a' ----P. a ,2 7-,- - 6 , i cn -q2- ❑ f, i 5 1 g 7.. g 21 t- 2 _,-. 1 . '1] ❑' a' '" ':;* ivi 2 d •a . Er > g 2 g "0 0, ❑ Sci- 9 g 2) m❑ 6 5 _-C- e7 a, = .,- = 0 6 , = - , = ,2 CI Fi :2: 5' us a " 8m06.o.s.co - .1. l'- , 05 1 -. 1 @,-, ,, 7 =' 0" = •, 5 - cs -%. 0 7 5 - a; ea r 0,-- ,c?, ss. E. „„. 0 0 001 - To „„ . Ei ',,--... r:g Q Lc w lni •--1' 5 '7 ° 8 ='" 5 -- -C 5- F - •c1 -, n a.. 0 La 0 a, 3 0.0 . 42 tD ,.,. a; > (1,- 8 D ..••• (Ty ...., OS 0 2 ,-* 3 8 d on 54. 5 '5' C 8 Eli 5* = c =4 c - o-- es .4. .7..'" = m C co Ch en (.5 e.-. CD = ,. --• 17i c ,-co---,0 ra. .,: - - co-`7r 7, °0• c" al a - 8 C3 n 3 2DI 13, F2.4 ,,, CD - Ei,-.: 0 0 - - 4 3 2. 9q0 8 c;50a . ca Ft . 6 C.() 5 . - CA 0 os 7.1 = a, -- =_ 5 5 e-,0 ;' co -. 5 ila ri) - 5 5 a FO' C L. 2 . 0 3 it, 5 ' ' 0 'V laa - NI © 8' 2 0 ..Z 3 - c . 0 5_. -., I. CD is. ,F z.o# ifi c o 2, 1 _.. .-, ,,, co 5. .... 5 wars g - E 3.elcg , 5 :a Qco - cn c'J 0 CO C .", 2 03 R 00 5- C4 A -, =, , ,, - n P'. z= - . " ... Id'- c90 m 0 .,., - '" 5 P. --- co c - ° Ck sv "5 P.- 2. ,,, c 0. IT z CD DI CD fa {D- 5 0 • s..,T NI ig ,- co, •. 3 '" 5 5 - {-13' ❑ n AD S. En - = c i- ,..., - 5' a = - .7.s. n115 5 .-=) z . n ...., --, a F- 0 C.... S3 3, 5. - a 0 _.co0ra = , c 0 5 R• 1:1 0 ,.. - = a; 4.: w a: cr; c2,, 2 -0 c n . o . F, Z 13 s. -, c11 ' -I cT: , c=„, a 5:4. LC - 7 .2Fri, m: a c . 0 15 8 - - 1 . -cm (I - o d -; 0 A C C - = 0) 0 W :!. n a CD to 5 ,.... Fli "C-5 . n E. = s...) as .7...; o 0) --- on _,. 0 -ti E- 5 - ,+ =. = .'''" Da ' ff- to Qc c 4 c la &I p. a. 5• ra - ' w .0 ❑ el 8 a ' 9 , 8' 5- n. r iz f`-' 0- 2 T*. 3@ 15. m - 55- 6 6T1 co 5 - n0,... -" .T.- .. --, -. c .=-° o - , .-- 0 a... -, a(a) d 0 5 g c:5• =• a - P-'- C5. m'. ti = e. 0 tu (5-g 0 al - -- m 0 0m - • 0 a _ .-% ... -ci ..4 -. 0 5' -1:1 -0 5. OD 5. 59, , c cp ...., 7 = co C2e CID 3 ,cc ci e •r1 3. 0. - a to et o c ca ❑ ZE 7 -- as-) c,., c. Qs -=0 aCD 0 ".' cr 0 CD 0 0 35t4 -' . a c- CQ g2:. . z -;.„ 5. 5 ,.., 0 IA as .< -. . ... ..fr: 0 . 0 50 3	INTERNATIONAL LAW for: applicability of international law to cyberspace NORMS CBM: universally agreed upon [voluntary] norms/rules/principles are important for the responsible behavior of States' use of ICTs STATE RESPONSIBILITY for: commit to nonproliferation activities related to cyber weapons

ID	Document	Document Groups	Quotation Content	Codes
185:5	2008 - Shanghai+Cooperation+Org Agreement	2008	0 -...2 , , 8'. ❑ '=-- 2 tl'i eD ' = 2 0 c 5 o _ ,-,-. .,-,1- .0. - -. .,, -1K > cL 0 7', 2 1r, 5 t: _, a. a cr JD (0 = co R -4 .-0 -Z,- .m ell .o. F, • 3 c.-D IS c :--.-=`.. 0 > 4 05 - za = - - c e5 47 Z ,=4. cz a) =- -s.) ,ep-k 3_ - Li 0 -- ----- - ...._..0__..=-74- -- 0-- ---- . in. 0 7'. 03 .-%--- ..-:---.--. z m_ - 7 q. .,...-.9 c-). --k- 0,:' ca---...-- c • ,..--.... .t.. 0 c ,--L- .-..m-'---irs- - - ...• ,. - -,....'a ,7,•' .-;_.. ;647 a) ca co co -'-, ----0 .--- _. c.,- ---- s s, (4,.1, it- 0 0 nc c 0 . r; '...) a. D - E- 3 2 ,,, -' al, E. (D CD L5 en 3al m 7 CO ,.... ' - -cl 7 '(8 >--1 cz 0 cl) 0 c- 5 y" -1 ❑ E 75' '" 4 a' ----P. a ,2 7-,- - 6 , i cn -q2- ❑ f, i 5 1 g 7.. g 21 t- 2 _,-. 1 . '1] ❑' a' '" ':;* ivi 2 d •a . Er > g 2 g "0 0, ❑ Sci- 9 g 2) m❑ 6 5 _-C- e7 a, = .,- = 0 6 , = - , = ,2 CI Fi :2: 5' us a " 8m06.o.s.co - .1. l'- , 05 1 -. 1 @,-, ,, 7 =' 0" = •, 5 - cs -%. 0 7 5 - a; ea r 0,-- ,c?, ss. E. „„. 0 0 001 - To „„ . Ei ',,--... r:g Q Lc w Ini •--1' 5 '7 ° 8 ='" 5 -- -C 5- F - •c1 -, n a.. 0 La 0 a, 3 0.0 . 42 tD ,,,. a; > (1,- 8 D ..••• (Ty ...., OS 0 2 ,-* 3 8 d on 54. 5 '5' C 8 Eli 5* = c =4 c - o-- es .4. .7..'" = m C co Ch en (.5 e.-. CD = ,. --• 17i c ,-co---,0 ra. .,: - - co-`7r 7, °0• c" al a - 8 C3 n 3 2DI 13, F2.4 ,,, CD - Ei,-.: 0 0 - - 4 3 2. 9q0 8 c;50a . ca Ft . 6 C.() 5 . - CA 0 os 7.1 = a, -- =_ 5 5 e-,0 ;' co -. 5 ila ri) - 5 5 a FO' C L. 2 . 0 3 it, 5 ' ' 0 'V laa - NI © 8' 2 0 ..Z 3 - c . 0 5_. -., I. CD is. ,F z.o# ifi c o 2, 1 _.. .-, ,,, co 5. .... 5 wars g - E 3.elcg , 5 :a Qco - cn c'J 0 CO C .", 2 03 R 00 5- C4 A -, =, , ,, - n P'. z= - . " ... Id'- c90 m 0 .,., - '" 5 P. --- co c - ° Ck sv "5 P.- 2. ,,, c 0. IT z CD DI CD fa {D- 5 0 • s..,T NI ig ,- co, •. 3 '" 5 5 - {-13' ❑ n AD S. En - = c i- ,..., - 5' a = - .7.s. n115 5 .-=) z . n ...., --, a F- 0 C.... S3 3, 5. - a 0 _.co0ra = , c 0 5 R• 1:1 0 ,.. - = a; 4.: w a: cr; c2,, 2 -0 c n . o . F, Z 13 s. -, c11 ' -I cT: , c=„ a 5:4. LC - 7 .2Fri, m: a c . 0 15 8 - - 1 . -cm (I - o d -; 0 A C C - = 0) 0 W :!. n a CD to 5 ,.... Fli "C-5 . n E. = s...) as .7...; o 0) --- on _,. 0 -ti E- 5 - ,+ =. = .'''" Da ' ff- to Qc c 4 c la &I p. a. 5• ra - ' w .0 ❑ el 8 a ' 9 , 8' 5- n. r iz f`-' 0- 2 T*. 3@ 15. m - 55- 6 6T1 co 5 - n0,... -" .T.- .. --, -. c .=-° o - , .-- 0 a... -, a(a) d 0 5 g c:5• =• a - P-'- C5. m'. ti = e. 0 tu (5-g 0 al - -- m 0 0m - • 0 a _ .-% ... -ci ..4 -. 0 5' -1:1 -0 5. OD 5. 59, , c cp ...., 7 = co C2e CID 3 ,cc ci e •r1 3. 0. - a to et o c ca ❑ ZE 7 -- as-) c,., c. Qs -=0 aCD 0 ".' cr 0 CD 0 0 35t4 -' . a c- CQ g2:. . z -;.„ 5. 5 ,.., 0 IA as .< -. . ... ..fr: 0 . 0 50 3 ,c = 0,1 .,.. um .,. a - a 0 ,.... ...4 cff m - 5 F [n • 7 co - .. (1 , co 0, CL Zi co . (0 M	CONFIDENCE BUILDING CBM: further investments in ICT research and development CYBER ATTACKS for: strengthen tools and resources needed to prepare, deter, defend, and respond to unlawful use of ICTs, cyber attacks / acts of cyber crime and/or terrorism INFORMATION EXCHANGE CBM: encourage further analysis and study by research institutes and universities on ICT security related matters STAKEHOLDER COOPERATION for: coordinate/cooperate in combatting cybercrime STAKEHOLDER COOPERATION for: work / intensify cooperation against criminal/terrorist use of ICTs
185:6	2008 - Shanghai+Cooperation+Org Agreement	2008	= co R -4 .-0 -Z,- .m ell .o. F, • 3 c.-D IS c :--.-=`.. 0 > 4 05 - za = - - c e5 47 Z ,=4. cz a) =- -s.) ,ep-k 3_ - Li 0 -- ----- - ...._..0__..=-74- -- 0-- ---- . in. 0 7'. 03 .-%--- ..-:---.--. z m_ - 7 q. .,...-.9 c-). --k- 0,:' ca---...-- c • ,..--.... .t.. 0 c ,--L- .-..m-'---irs- - - ...• ,. - -,....'a ,7,•' .-;_.. ;647 a) ca co co -'-, ----0 .--- _. c.,- ---- s s, (4,.1, it- 0 0 nc c 0 . r; '...) a. D - E- 3 2 ,,, -' al, E. (D CD L5 en 3al m 7 CO ,.... ' - -cl 7 '(8 >--1 cz 0 cl) 0 c- 5 y" -1 ❑ E 75' '" 4 a' ----P. a ,2 7-,- - 6 , i cn -q2- ❑ f, i 5 1 g 7.. g 21 t- 2 _,-. 1 . '1] ❑' a' '" ':;* ivi 2 d •a . Er > g 2 g "0 0, ❑ Sci- 9 g 2) m❑ 6 5 _-C- e7 a, = .,- = 0 6 , = - , = ,2 CI Fi :2: 5' us a " 8m06.o.s.co - .1. l'- , 05 1 -. 1 @,-, ,, 7 =' 0" = •, 5 - cs -%. 0 7 5 - a; ea r 0,-- ,c?, ss. E. „„. 0 0 001 - To „„ . Ei ',,--... r:g Q Lc w Ini •--1' 5 '7 ° 8 ='" 5 -- -C 5- F - •c1 -, n a.. 0 La 0 a, 3 0.0 . 42 tD ,,,. a; > (1,- 8 D ..••• (Ty ...., OS 0 2 ,-* 3 8 d on 54. 5 '5' C 8 Eli 5* = c =4 c - o-- es .4. .7..'" = m C co Ch en (.5 e.-. CD = ,. --• 17i c ,-co---,0 ra. .,: - - co-`7r 7, °0• c" al a - 8 C3 n 3 2DI 13, F2.4 ,,, CD - Ei,-.: 0 0 - - 4 3 2. 9q0 8 c;50a . ca Ft . 6 C.() 5 . - CA 0 os 7.1 = a, -- =_ 5 5 e-,0 ;' co -. 5 ila ri) - 5 5 a FO' C L. 2 . 0 3 it, 5 ' ' 0 'V laa - NI © 8' 2 0 ..Z 3 - c . 0 5_. -., I. CD is. ,F z.o# ifi c o 2, 1 _.. .-, ,,, co 5. .... 5 wars g - E 3.elcg , 5 :a Qco - cn c'J 0 CO C .", 2 03 R 00 5- C4 A -, =, , ,, - n P'. z= - . " ... Id'- c90 m 0 .,., - '" 5 P. --- co c - ° Ck sv "5 P.- 2. ,,, c 0. IT z CD DI CD fa {D- 5 0 • s..,T NI ig ,- co, •. 3 '" 5 5 - {-13' ❑ n AD S. En - = c i- ,..., - 5' a = - .7.s. n115 5 .-=) z . n ...., --, a F- 0 C.... S3 3, 5. - a 0 _.co0ra = , c 0 5 R• 1:1 0 ,.. - = a; 4.: w a: cr; c2,, 2 -0 c n . o . F, Z 13 s. -, c11 ' -I cT: , c=„ a 5:4. LC - 7 .2Fri, m: a c . 0 15 8 - - 1 . -cm (I - o d -; 0 A C C - = 0) 0 W :!. n a CD to 5 ,.... Fli "C-5 . n E. = s...) as .7...; o 0) --- on _,. 0 -ti E- 5 - ,+ =. = .'''" Da ' ff- to Qc c 4 c la &I p. a. 5• ra - ' w .0 ❑ el 8 a ' 9 , 8' 5- n. r iz f`-' 0- 2 T*. 3@ 15. m - 55- 6 6T1 co 5 - n0,... -" .T.- .. --, -. c .=-° o - , .-- 0 a... -, a(a) d 0 5 g c:5• =• a - P-'- C5. m'. ti = e. 0 tu (5-g 0 al - -- m 0 0m - • 0 a _ .-% ... -ci ..4 -. 0 5' -1:1 -0 5. OD 5. 59, , c cp ...., 7 = co C2e CID 3 ,cc ci e •r1 3. 0. - a to et o c ca ❑ ZE 7 -- as-) c,., c. Qs -=0 aCD 0 ".' cr 0 CD 0 0 35t4 -' . a c- CQ g2:. . z -;.„ 5. 5 ,.., 0 IA as .< -. . ... ..fr: 0 . 0 50 3 ,c = 0,1 .,.. um .,. a - a 0 ,.... ...4 cff m - 5 F [n • 7 co - .. (1 , co 0, CL Zi co	CRITICAL INFRASTRUCTURE for: protecting critical infrastructures STAKEHOLDER COOPERATION for: coordinate/cooperate in preserving multistakeholder internet governance

ID	Document	Document Groups	Quotation Content	Codes
185:7	2008 - Shanghai+Cooperation+Org Agreement	2008	0 c 5 o _ ,-,-. .,-,1- .0. - -. .,, -1K > cL 0 7', 2 1r, 5 t: _, a. a cr JD (0 = co R -4 .-0 -Z,- .m ell .o. F, • 3 c.-D IS c :--.-=`.. 0 > 4 05 - za = - - c e5 47 Z ,=4. cz a) =- -s.) ,ep-k 3_ - Li 0 -- ----- - ...._..0__..=-74- - - 0-- ---- . in. 0 7'. 03 .-%--- ..-:---.--. z m_ - 7 q. .,...-.9 c-). --k- 0,:' ca---...-- c • ,..--.... .t.. 0 c ,--L- .-..m- '---irs- - - ...• ,. - -,....'a ,7,•' .-;_.. ;647 a) ca co co -'-, ----0 .--- _. c.,- ---- s s, (4,.1, it- 0 0 nc c 0 . r; '...) a. D - E- 3 2 ,,, -' al, E. (D CD L5 en 3al m 7 CO ,.... ' - -cl 7 '(8 >--1 cz 0 cl) 0 c- 5 y" -1 ❑ E 75' '" 4 a' - ---P. a ,2 7-,- - 6 , i cn -q2- ❑ f, i 5 1 g 7.. g 21 t- 2 _,-. 1 . '1] ❑' a' "' ':;* ivi 2 d •a . Er > g 2 g "0 0, ❑ Sci- 9 g 2) m❑ 6 5 _-C- e7 a, = .,- = 0 6 , = - , = ,2 CI Fi :2: 5' us a " 8m06.o.s.co - .1. l'- , 05 1 -. 1 @,-, ,, 7 =' 0" = •, 5 - cs -%. 0 7 5 - a; ea r 0,-- ,c?, ss. E. „„. 0 0 001 - To „„ . Ei ',,--... r:g Q Lc w lni •--1' 5 '7 ° 8 ='" 5 -- -C 5- F - •c1 -, n a.. 0 La 0 a, 3 0.0 . 42 tD ,.,. a; > (1,- 8 D ..••• (Ty ...., OS 0 2 ,-* 3 8 d on 54. 5 '5' C 8 Eli 5* = c =4 c - o-- es .4. .7..'" = m C co Ch en (.5 e.-. CD = ,. --• 17i c ,-co---,0 ra. .,: - - co-`7r 7, °0• c" al a - 8 C3 n 3 2DI 13, F2.4 ,,, CD - Ei,-.: 0 0 - - 4 3 2. 9q0 8 c;50a . ca Ft . 6 C.() 5 . - CA 0 os 7.1 = a, -- =_ 5 5 e-,0 ;' co -. 5 ila ri) - 5 5 a FO' C L. 2 . 0 3 it, 5 ' ' 0 'V laa - NI © 8' 2 0 ..Z 3 - c . 0 5_. -., I. CD is. ,F z.o# ifi c o 2, 1 _.. .-, ,,, co 5. .... 5 wars g - E 3.elcg , 5 :a Qco - cn c'J 0 CO C .", 2 03 R 00 5- C4 A -, =, , ,, - n P'. z= - . " ... Id'- c90 m 0 .,., - '" 5 P. --- co c - ° Ck sv "5 P.- 2. ,,, c 0. IT z CD DI CD fa {D- 5 0 • s..,T NI ig ,- co, •. 3 '" 5 5 - {-13' ❑ n AD S. En - = c i- ,..., - 5' a = - .7.s. n115 5 .-=) z . n ...., --, a F- 0 C.... S3 3, 5. - a 0 _.co0ra = , c 0 5 R• 1:1 0 ,.. - = a; 4.: w a: cr; c2,, 2 -0 c n . o . F, Z 13 s. -, c11 ' -I cT: , c=„, a 5:4. LC - 7 .2Fri, m: a c . 0 15 8 - - 1 . -cm (I - o d -; 0 A C C - = 0) 0 W :!. n a CD to 5 ,.... Fli "C-5 . n E. = s...) as .7...; o 0) --- on _,. 0 -ti E- 5 - ,+ =. = .""" Da ' ff- to Qc c 4 c la &l p. a. 5• ra - ' w .0 ❑ el 8 a ' 9 , 8' 5- n. r iz f`-' 0- 2 T*. 3@ 15. m - 55- 6 6T1 co 5 - n0,... -" .T.- .. --, -. c .=-° o - , .-- 0 a... -, a(a) d 0 5 g c:5• =• a - P-'- C5. m'. ti = e. 0 tu (5-g 0 al - -- m 0 0m - • 0 a _ .-% ... -ci ..4 -. 0 5' -1:1 -0 5. OD 5. 59, , c cp ...., 7 = co C2e CID 3 ,cc ci e •r1 3. 0. - a to et o c ca ❑ ZE 7 -- as-) c,., c. Qs -=0 aCD 0 ".' cr 0 CD 0 0 35t4 -' . a c- CQ g2:. . z -;.„ 5. 5 ,.., 0 IA as .< -. . ... ..fr: 0 . 0 50 3 ,c = 0,1 .,.. um .,. a - a 0 ,.... ...4 cff m - 5 F [n • 7 co - .. (1 , co 0, C	INFORMATION EXCHANGE for: sharing information regarding national laws/policies/rules/regulations regarding ICTs/cyber space/cybersecurity NORMS proposal: enhance and further elaborate of norms
185:8	2008 - Shanghai+Cooperation+Org Agreement	2008	a ,' . 0. - ,.., _ -, co c ro 7, ca: tt; v, 3 cu -2 60 0 0 ca," u'5 m- coct Co -, ,-. . ,..,- CD -• N3 n iii =in ,.. = = sl&- 0 0n-al rD. •-g>c-grc"-al In __ -, -". -; 0 c m 7-7.= CO 1)0m ps o 0.. =as 0 0,-. - c . - o_ co gyi - =N• fi- 5' -, .• - = = 94 c = 1 c)33.=0-cp.,3 .i9 4" 0carnm -- is- ._, - -.. ,<0 cooD - E 1- -' C) > = 0zi F: 07.<a. 20 --, fa c E D- ,-- 0 . 5 F.J 3r3 0.... 0 -6. cci ai ,r. c.ri n ., g -.: .,•, . CZ' =, - * CD 1 .7. . a h c2 e f 1 , ., . , - , . „ . . o a oo to w.i; - .,. ,,, n, _ g.. 5' = 0 9. , , co J a. co cc -,,,, , - , 0 c .... _ -, E .„ „, „ - --, 0 cr c- ". = .„._ =,- c E ,5 .i...0 , , 0 9., 0 n , 0 w hj a) .... =, -; cl " w' ,.,. -5 2 ---= -i5 .- = ' . = = 3 .- 'a CL Fd P it 14 E CD D.- R 5 3 c!) cn . a c S. r`4 =. (A o) an '" 1::( EF --, - L 0-. °-r.7.. .:1 L-- .. 3 o• 0 - 5 (0 a.vm5 0= 0 ro. 5 c-n . :..-, CD 0P-3 ,-, 0 6 -rl d,' ' ,dj, v„ . Sl.- ' gn) a c1 113 - --` 0 8- CD <-7) W 5 a' - 80 ,72-.2P0-zr m,-5 ,;,, o ,.e" 5. 42' tr Fr 2ct-2.a[a.3-.5c11-5 " S c. !el 8 8 P., r-r, -5 -60ci, c x0 rci 2 41 ,.,/,1 ---..tLIR,50'qJ3=-' -__-, = Q. a os 5 = a < = •-0 -i .3 6- x-5,' -e(D-D' n - . t ;c:ET m 'a fa al 5' 0 p ,-c- -0 cn m o a -03--. w ro ril - z co „ uost- ,,,--- -L7/3 - 6 8" 94 10 ci ...,.. =. cn .-4. -ro_80 -c - = ' ' c •- • 'c -,.3 - 9,, ' 5' 1;.•-7,--9-, r= = m,coS-0li - -'". Cd .". 05-=c1,.., c-) iF_a 80 0'=kn 1Li, 6 co .0 7 ro E.'L5 - 0 - c •r2Rem-0 =. R co •Z m 8 ' c.D:D.,1 -5 A.4-., . •t. • . , ■-3• Cr IC - g 7 rc, (r 2 C 0 m.z^"cia== 7" °' "; ' . -1 5 :..---. c ,.,1 -o cc, 5, „T gl, c ff -0 c 5 2 Ali -0 0 CI = .., -. 0 g 5 c 5. os ca ,. ....m.-.. I.•• 0 L IJ = t c. ,3 •-1, .74, (I -0 - ..... •-•- ... aD ea _ n .,-. , cD ca , -. „ -• ro,, am 0 - o ':.4. 50 - '1D ='-. c c. z co 5 r71. . c'- 14 GI. ilfa D 'E I c- k ,?: g 5-3 , ay us ti7 0 al 6.-- -0 . ;0 5L., C6 2 4 4 a .= 9 -._ ... cr- g Eau co 0 -k 0, i:3: ,, c,,,- •• C 5.EcTiR,-wm rA -5' ❑DI =, w - c C) ,t -3. --:-- E... cA g.th :• 2 9 = 0 cER. -, _ _., a fa 6, cV 71 CA. a- 5. C13 0.7 5 _,- . Ir, on . .14- , (13 ....- al , L'. = 0. _. ,9_ i)• - g ❑ co , 5. FP 2 10. 2 '" . :513 Cil - - S -8 „ , 'D - - o 3, : Zi .52. 11. '" o0c-.co,>0r)=0 c6 - m la 0 c,7, 0 ... CD Er * 2 g25 - clE'....=4 5' ca ,., ,Rctm --- Ei '-rAE - (01 ,-.. 5_- 0sng .5, -.- a) 0.0 0 ci ❑ In 9, r irD, -' ^ . rn .., _. nz ,-, 9 8_,-, ., co a= 0 by .6 - Pj, .5 ,Cr c.5 ce;, 00 7,,' a al e0 L _ -0 7 c0 Cil -01' •C DI CD • 9„ - ,cp, w di , CD 012 6 i.a c- .0 w = 23 EA aq -tr 1.1i -. ' a E cD. = ' '" ti) -, .4. ,,,, ,.... .1.1 d2 0 _ _, n a, 7D Cr, 5 rli ,.,., . 71 71 _ = Cr ir, = a 0 .- co 1:3 cr ° °IR 8- - c' ' '"" 6. 7= Z-. CO = 2 ti:! g C "" . n Ca Cy 3 B,' ". g `6 -3 8 a3 o- i.7, 0 ° Gt. as 2, g=4/7Ca.= rg r '... 5• c,66, `3 cn ca F T a 5-:6'. 7,.. c< v..; cPc'o)coco=0 ' 4.. ' _R ❑ ,... -0 v.; r0 E t6 vi 15 0 0.1c.9.. - .« =· . 0c= _ o ,,,, 0063 . .., . a .r. .-e... E 4 3 ; E P =. 03 rz.- in -71 0 t - c - -I ' .v, -.: aL 0 8 _-,n _ -cac°16 Ez - > 4 R -_,_ '..*- CI) 7' R-- W `-4n, g 5 co El Pi 0 co 0 ' =• C-'- 8 - E. = m 0) q m- ❑ Ft 7h roRSS Fs 4:2 ❑ . Rg s3 - ?_2-. E 2. > -.?...: a --, ,-, cil __. 5. 7.; c __ cl ,,, 0 -- co a- = c u] -e 0 5ct--La -' ❑ = c z- =.- 7--7g5;c:.-. • - •--4- 77..-. w075c _.._al,., 1 c.,4,4',355- .E.,..,.vic . ❑ al a 6- 2 2 g 0 9 m ES 0 LS: C el) -L. , 0 1:1 M J. = " ..2 ' a '1- 11. 8 7 a F' 8	INFORMATION EXCHANGE for: sharing of good/best practices in relation to ICTs and cybersecurity NORM for: promote cooperation in training to develop ICT/cybersecurity awareness and skills

ID	Document	Document Groups	Quotation Content	Codes
186:1	2007 - IGF Chairman Summary.FINAL.16.11.2007	2007	here were seven main sessions in an innovative format of interactive multi-stakeholder panels with questions and comments from the audience. T	STAKEHOLDER COOPERATION for: coordinate/cooperate in preserving multistakeholder internet governance
186:2	2007 - IGF Chairman Summary.FINAL.16.11.2007	2007	In terms of participants, there were over 2,100 registered participants prior to the meeting, of which 700 came from civil society, 550 from government, 300 from business entities, 100 from international organizations, and 400 representing other categories. The meeting was attended by 1,363 participants from 109 countries. Additionally, over 100 members of the press attended the event. These statistics can be viewed on the IGF Web site at - www.intgovforum.org/stats.php	INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information STAKEHOLDER COOPERATION for: encourage participation of other stakeholders such as the private sector, academia, and civil society orgs (as appropriate) for CBM and/or norm creation and implementation
186:3	2007 - IGF Chairman Summary.FINAL.16.11.2007	2007	With regard to the economic dimension, there was a discussion on market dominance and virtual monopolies and their relationship to openness and freedom of expression. It was also pointed out that the discussion in the IGF had a relationship to discussions held in the World Intellectual Property Organization, in particular with regard to its Development Agenda, and UNESCO with regard to the Convention on the Protection and Promotion of the Diversity of Cultural Expression	STAKEHOLDER COOPERATION for: support other international and/or regional cooperative partnerships
186:4	2007 - IGF Chairman Summary.FINAL.16.11.2007	2007	While some called for more legislation, there was also a warning against over-regulation. Many speakers pointed out that collaborative, multi-stakeholder efforts of cooperation could be sufficient. The forum noted that both hard law and soft law solutions were needed to enhance security. There was a strong call for harmonizing legislation between countries and also for bringing into force new legal instruments that apply to the on-line world. The Council of Europe Convention on Cybercrime was mentioned as a promising approach that more nations should adopt	CONFIDENCE BUILDING CBM: adopt legislative basis for combatting cybercrime (i.e., the Budapest Convention) STAKEHOLDER COOPERATION for: coordinate/cooperate in combatting cybercrime STATE RESPONSIBILITY for: adhering to rules and regulations agreed upon by previously enacted international law/mandates/treaties
186:5	2007 - IGF Chairman Summary.FINAL.16.11.2007	2007	As had been echoed in a number of other IGF sessions, one panellist remarked that it was essential to build up community infrastructures, including critical Internet resources, in order to reach the five and a half billion people in the world who did not have access to the Interne	ACCESS CBM: access to the internet is an important enabler of development./growth/innovation CRITICAL INFRASTRUCTURE for: promoting resilience (as related to ICTs,cybersecurity, and related critical infrastructure
186:6	2007 - IGF Chairman Summary.FINAL.16.11.2007	2007	The panel and the discussion gave a strong emphasis on the fundamental freedoms, the freedom of expression and the free flow of information, as contained in Article 19 of the Universal Declaration of Human Rights and the Geneva Declaration of Principles and the Tunis Agenda in the WSIS context. It was pointed out that a human rights perspective should go beyond paying lip service to these universally accepted principles.	ACCESS CBM: creating a free flow of and acccess to the internet is essential for the digital economy, and beneficial to development ACCESS for: support the free flow of information while respecting applicable legal frameworks for privacy and data protection CONFIDENCE BUILDING for: ensuring the free flow of data while also protecting the integrity of that data and the privacy of individual users HUMAN RIGHTS for: respecting human rights and fundamental freedoms; applying them to cyber space / ICT use, etc.
186:7	2007 - IGF Chairman Summary.FINAL.16.11.2007	2007	Another panellist spoke of the effort to create a national IGF following the multi-stakeholder model. She also spoke of the success of self regulation in the UK and indicated that while critical Internet resources were not a critical issue for users, security issues as well as issues of access in developing counties were important.	ASSIST for: adopting appropriate policies and measures so that developing countries benefit from the advantages of technological progress (and do not suffer from lack of early adoption) ASSISTANCE CBM: provide assistance and training to developing countries to improve cybsecurity and ICT use
187:1	2006 - IGF 2006 Summary.Final.07.11.2006	2006	There were six panel sessions in an innovative format of interactive multi-stakeholder panels with questions and comments from the audience. Remote participants were given the opportunity to take part via blogs, chat rooms, email and text messaging.	STAKEHOLDER COOPERATION CBM: states should participate and cooperate in multilateral forums STAKEHOLDER COOPERATION for: coordinate/cooperate in preserving multistakeholder internet governance
187:2	2006 - IGF 2006 Summary.Final.07.11.2006	2006	The Openness session focused on free flow of information and freedom information on the one hand and access to information and knowledge on the other. Much of the discussion was devoted to finding the right balance: • the balance between freedom of expression and responsible use of this freedom; and • the balance between protecting copyright and access to knowledge.	ACCESS CBM: access to the internet is an important enabler of development./growth/innovation ACCESS CBM: creating a free flow of and acccess to the internet is essential for the digital economy, and beneficial to development ACCESS for: support the free flow of information while respecting applicable legal frameworks for privacy and data protection CONFIDENCE BUILDING for: ensuring the free flow of data while also protecting the integrity of that data and the privacy of individual users INFORMATION EXCHANGE for: furthering future dialogue/cooperation for a safe, open, and secure internet/cyberspace NORM for: promote an open, secure, stable, accessible, and peaceful cyber space / ICT environment
187:3	2006 - IGF 2006 Summary.Final.07.11.2006	2006	The role of the IGF in collating best practices, ensuring the widespread dissemination of information and breaking down 'silo' approaches to the problem were all highlighted. The ability of the IGF to support the development of a common language in the policy debate was seen as very significant	INFORMATION EXCHANGE for: sharing of good/best practices in relation to ICTs and cybersecurity

ID	Document	Document Groups	Quotation Content	Codes
187:4	2006 - IGF 2006 Summary.Final.07.11.2006	2006	A representative from UNESCO drew attention to the Universal Declaration on Cultural Diversity mentioning that its purpose was to support the expressions of culture and identity through the diversity of language	STATE RESPONSIBILITY for: adhering to rules and regulations agreed upon by previously enacted international law/mandates/treaties
187:5	2006 - IGF 2006 Summary.Final.07.11.2006	2006	One suggestion is to establish multistakeholder cooperation between the various institutions dealing with these issues, such as UNESCO, ITU, ICANN and ISOC/IETF, to come up with solutions	STAKEHOLDER COOPERATION for: support other international and/or regional cooperative partnerships
187:6	2006 - IGF 2006 Summary.Final.07.11.2006	2006	Several participants also spoke about a gender divide within the digital divide. It was mentioned that frequently access in the developing world had a gender bias insofar as efforts were oriented more towards the boys than girls. This was seen by some participants as an additional problem in that it makes the gender divide worse in places where the digital divide was being alleviated.	DIGITAL EQUALITY for: closing the digital divide (i.e., by empowering communities to benefit from digital opportunities) DIGITAL EQUALITY for: closing the gender digital divide (focusing on women and girls, but also those a part of gender subgroups such as the LGBTQI+ communiy)
187:7	2006 - IGF 2006 Summary.Final.07.11.2006	2006	A number of panelists spoke about the way the Internet enables citizens to become educated and aware of some of the conditions that affected their lives. This was seen as a major contribution to strengthening democracy.	EDUCATE AND STRENGTHEN THE GENERAL PUBLIC for: providing users/customers/the general public with information and tools that will enable them to understand current and future threats, as well as protect against them EDUCATION CBM: skills development, particularly for younger individuals (both internal and external, international and/or domestic) EDUCATION for: educating users/customers on how their data may be used, and how to protect it EDUCATION for: increased eduation, [digital] literacy, and awareness regarding digital rights and ways to exercise/protect them
188:1	2005 - UN WSIS_ Geneva Declaration of Principles	2005	We, the representatives of the peoples of the world, assembled in Geneva from 10-12 December 2003 for the first phase of the World Summit on the Information Society, declare our common desire and commitment to build a people-centred, inclusive and development-oriented Information Society, where everyone can create, access, utilize and share information and knowledge, enabling individuals, communities and peoples to achieve their full potential in promoting their sustainable development and improving their quality of life, premised on the purposes and principles of the Charter of the United Nations and respecting fully and upholding the Universal Declaration of Human Rights	HUMAN RIGHTS for: respecting human rights and fundamental freedoms; applying them to cyber space / ICT use, etc. STAKEHOLDER COOPERATION CBM: states should participate and cooperate in multilateral forums STATE RESPONSIBILITY for: adhering to rules and regulations agreed upon by previously enacted international law/mandates/treaties
188:2	2005 - UN WSIS_ Geneva Declaration of Principles	2005	n keeping with the spirit of this declaration, we rededicate ourselves to upholding the principle of the sovereign equality of all States.	INTERNATIONAL LAW for: applicability of international law to cyberspace STATE SOVEREIGNTY for: state sovereignty applied to State's ICT activities & ICT infrastructure within their territory
188:3	2005 - UN WSIS_ Geneva Declaration of Principles	2005	We are fully committed to turning this digital divide into a digital opportunity for all, particularly for those who risk being left behind and being further marginalized.	DIGITAL EQUALITY for: closing the digital divide (i.e., by empowering communities to benefit from digital opportunities) DIGITAL EQUALITY for: closing the gender digital divide (focusing on women and girls, but also those a part of gender subgroups such as the LGBTQI+ communiy)
188:4	2005 - UN WSIS_ Geneva Declaration of Principles	2005	They must therefore be empowered as learners, developers, contributors, entrepreneurs and decision-makers. We must focus especially on young people who have not yet been able to benefit fully from the opportunities provided by ICTs. We are also committed to ensuring that the development of ICT applications and operation of services respects the rights of children as well as their protection and well-being.	EDUCATION CBM: skills development, particularly for younger individuals (both internal and external, international and/or domestic)
188:5	2005 - UN WSIS_ Geneva Declaration of Principles	2005	We continue to pay special attention to the particular needs of people of developing countries, countries with economies in transition, Least Developed Countries, Small Island Developing States, Landlocked Developing Countries, Highly Indebted Poor Countries, countries and territories under occupation, countries recovering from conflict and countries and regions with special needs as well as to conditions that pose severe threats to development, such as natural disasters.	ASSIST for: adopting appropriate policies and measures so that developing countries benefit from the advantages of technological progress (and do not suffer from lack of early adoption) ASSISTANCE CBM: provide assistance and training to developing countries to improve cybsecurity and ICT use STAKEHOLDER COOPERATION CBM: civil society is important when developing research, coordinating, and collaborating in understanding key and emerging gender-related issues

ID	Document	Document Groups	Quotation Content	Codes
188:6	2005 - UN WSIS_ Geneva Declaration of Principles	2005	Governments, as well as private sector, civil society and the United Nations and other international organizations have an important role and responsibility in the development of the Information Society and, as appropriate, in decision-making processes. Building a people-centred Information Society is a joint effort which requires cooperation and partnership among all stakeholders.	STAKEHOLDER COOPERATION for: coordinate/cooperate in preserving multistakeholder internet governance STAKEHOLDER COOPERATION for: encourage participation of other stakeholders such as the private sector, academia, and civil society orgs (as appropriate) for CBM and/or norm creation and implementation STAKEHOLDER COOPERATION for: recognizing the private sector's responsibilities in working towards improving trust, security, and stability in cyberspace
188:7	2005 - UN WSIS_ Geneva Declaration of Principles	2005	The ability for all to access and contribute information, ideas and knowledge is essential in an inclusive Information Society. 25. The sharing and strengthening of global knowledge for development can be enhanced by removing barriers to equitable access to information for economic, social, political, health, cultural, educational, and scientific activities and by facilitating access to public domain information, including by universal design and the use of assistive technologies.	ACCESS CBM: access to the internet is an important enabler of development./growth/innovation
188:8	2005 - UN WSIS_ Geneva Declaration of Principles	2005	We strive to promote universal access with equal opportunities for all to scientific knowledge and the creation and dissemination of scientific and technical information, including open access initiatives for scientific publishing.	NORM for: promote an open, secure, stable, accessible, and peaceful cyber space / ICT environment
188:9	2005 - UN WSIS_ Geneva Declaration of Principles	2005	The use of ICTs in all stages of education, training and human resource development should be promoted, taking into account the special needs of persons with disabilities and disadvantaged and vulnerable groups. 11/30/2020 WSIS: Declaration of Principles www.itu.int/net/wsis/docs/geneva/official/dop.html 4/7 31. Continuous and adult education, re-training, life-long learning, distance-learning and other special services, such as telemedicine, can make an essential contribution to employability and help people benefit from the new opportunities offered by ICTs for traditional jobs, self-employment and new professions. Awareness and literacy in ICTs are an essential foundation in this regard. 32. Content creators, publishers, and producers, as well as teachers, trainers, archivists, librarians and learners, should play an active role in promoting the Information Society, particularly in the Least Developed Countries.	CAPACITY BUILDING CBM: assign appropriate weight to ICT security awareness and capacity building in development and assistance planning CAPACITY BUILDING CBM: develop strategies for sustanability in ICT security (capacity-building) CAPACITY BUILDING CBM: encourage further work in capacity-building
188:10	2005 - UN WSIS_ Geneva Declaration of Principles	2005	Strengthening the trust framework, including information security and network security, authentication, privacy and consumer protection, is a prerequisite for the development of the Information Society and for building confidence among users of ICTs. A global culture of cyber-security needs to be promoted, developed and implemented in cooperation with all stakeholders and international expert bodies. These efforts should be supported by increased international cooperation. Within this global culture of cyber- security, it is important to enhance security and to ensure the protection of data and privacy, while enhancing access and trade. In addition, it must take into account the level of social and economic development of each country and respect the development-oriented aspects of the Information Society. 36. While recognizing the principles of universal and non-discriminatory access to ICTs for all nations, we support the activities of the United Nations to prevent the potential use of ICTs for purposes that are inconsistent with the objectives of maintaining international stability and security, and may adversely affect the integrity of the infrastructure within States, to the detriment of their security. It is necessary to prevent the use of information resources and technologies for criminal and terrorist purposes, while respecting human rights. 37. Spam is a significant and growing problem for users, networks and the Internet as a whole. Spam and cyber-security should be dealt with at appropriate national and international levels.	CONFIDENCE BUILDING CBM: CBM are important for increasing transparency, predictability, and stability CONFIDENCE BUILDING CBM: voluntary transparency CONFIDENCE BUILDING for: CBMs' value in increasing transparency, predictability, and stability CONFIDENCE BUILDING for: enhance trust,, confidence, and cooperation regarding ICTs, cyberspace and cybersecurity CYBER STABILITY for: maintaining a secure, safe, and trustable ICT environment
188:11	2005 - UN WSIS_ Geneva Declaration of Principles	2005	Regional integration contributes to the development of the global Information Society and makes strong cooperation within and among regions indispensable. Regional dialogue should contribute to national capacity building and to the alignment of national strategies with the goals of this Declaration of Principles in a compatible way, while respecting national and regional particularities. In this context, we welcome and encourage the international community to support the ICT-related measures of such initiatives.	CAPACITY BUILDING CBM: develop regional approaches to capacity-building CONFIDENCE BUILDING for: promote cooperation in regional confidence-building measures (CBMs) STAKEHOLDER COOPERATION for: support other international and/or regional cooperative partnerships

ID	Document	Document Groups	Quotation Content	Codes
190:1	2005 - UN WSIS Tunis Commitment	2005	1. We, the representatives of the peoples of the world, have gathered in Tunis from 16-18 November 2005 for this second phase of the World Summit on the Information Society (WSIS) to reiterate our unequivocal support for the Geneva Declaration of Principles and Plan of Action adopted at the first phase of the World Summit on the Information Society in Geneva in December 2003. 2. We reaffirm our desire and commitment to build a people-centred, inclusive and development-oriented Information Society, premised on the purposes and principles of the Charter of the United Nations, international law and multilateralism, and respecting fully and upholding the Universal Declaration of Human Rights, so that people everywhere can create, access, utilize and share information and knowledge, to achieve their full potential and to attain the internationally agreed development goals and objectives, including the Millennium Development Goals.	HUMAN RIGHTS for: respecting human rights and fundamental freedoms; applying them to cyber space / ICT use, etc. INTERNATIONAL LAW for: applicability of international law to cyberspace STAKEHOLDER COOPERATION CBM: states should participate and cooperate in multilateral forums STATE RESPONSIBILITY for: adhering to rules and regulations agreed upon by previously enacted international law/mandates/treaties UNITED NATIONS CBM: the United Nations (UN) may serve as an international body for decision-making, framework creation/implementation, and when developing and adopting universally agreed upon ICT norms/rules/principles (in order to ensure peace and responsible behavior/ICT use)
190:2	2005 - UN WSIS Tunis Commitment	2005	6. This Summit is an important stepping-stone in the world's efforts to eradicate poverty and to attain the internationally agreed development goals and objectives, including the Millennium Development Goals. By the Geneva decisions, we established a coherent long-term link between the WSIS process, and other relevant major United Nations conferences and summits. We call upon governments, private sector, civil society and international organizations to join together to implement the commitments set forth in the Geneva Declaration of Principles and Plan of Action. In this context, the outcomes of the recently concluded 2005 World Summit on the review of the implementation of the Millennium Declaration are of special relevance	STAKEHOLDER COOPERATION for: coordinate/cooperate in preserving multistakeholder internet governance STAKEHOLDER COOPERATION for: encourage participation of other stakeholders such as the private sector, academia, and civil society orgs (as appropriate) for CBM and/or norm creation and implementation
190:3	2005 - UN WSIS Tunis Commitment	2005	to boost literacy and universal primary education, and to facilitate the learning process itself, thus laying the groundwork for the establishment of a fully inclusive and development-oriented Information Society and knowledge economy which respects cultural and linguistic diversity	EDUCATION CBM: skills development, particularly for younger individuals (both internal and external, international and/or domestic) EDUCATION for: increased eduation, [digital] literacy, and awareness regarding digital rights and ways to exercise/protect them
190:4	2005 - UN WSIS Tunis Commitment	2005	14. We also recognize that in addition to building ICT infrastructure, there should be adequate emphasis on developing human capacity and creating ICT applications and digital content in local language, where appropriate, so as to ensure a comprehensive approach to building a global Information Society	CRITICAL INFRASTRUCTURE for: protecting critical infrastructures
190:5	2005 - UN WSIS Tunis Commitment	2005	13. We also recognize that the ICT revolution can have a tremendous positive impact as an instrument of sustainable development. In addition, an appropriate enabling environment at national and international levels could prevent increasing social and economic divisions, and the widening of the gap between rich and poor countries, regions, and individuals—including between men and women.	DIGITAL EQUALITY for: closing the digital divide (i.e., by empowering communities to benefit from digital opportunities) DIGITAL EQUALITY for: closing the gender digital divide (focusing on women and girls, but also those a part of gender subgroups such as the LGBTQI+ communiy)
190:6	2005 - UN WSIS Tunis Commitment	2005	Society, we underscore that ICTs are effective tools to promote peace, security and stability, to enhance democracy, social cohesion, good governance and the rule of law, at national, regional and international levels. ICTs can be used to promote economic growth and enterprise development. Infrastructure development, human capacity building, information security and network security are critical to achieve these goals. We further recognize the need to effectively confront challenges and threats resulting from use of ICTs for purposes that are inconsistent with objectives of maintaining international stability and security and may adversely affect the integrity of the infrastructure within States, to the detriment of their security. It is necessary to prevent the abuse of information resources and technologies for criminal and terrorist purposes, while respecting human rights	DIGITAL GOVERNANCE for: future digital [global] governance should be value-based, inclusive, open, and transparent INFORMATION EXCHANGE for: furthering future dialogue/cooperation for a safe, open, and secure internet/cyberspace NORM for: promote an open, secure, stable, accessible, and peaceful cyber space / ICT environment
190:7	2005 - UN WSIS Tunis Commitment	2005	21. To that end, we shall pay special attention to the particular needs of people of developing countries, countries with economies in transition, Least Developed Countries, Small Island Developing States, Landlocked Developing Countries, Highly Indebted Poor Countries, countries and territories under occupation, and countries recovering from conflict or natural disasters.	ASSIST for: adopting appropriate policies and measures so that developing countries benefit from the advantages of technological progress (and do not suffer from lack of early adoption) ASSISTANCE CBM: provide assistance and training to developing countries to improve cybsecurity and ICT use

ID	Document	Document Groups	Quotation Content	Codes
192:1	2005 - UN WGIG REPORT	2005	The WGIG first considered five criteria, namely that the working definition should be adequate, generalizable, descriptive, concise and process-oriented. Second, the WGIG analysed a wide range of public-sector, private-sector and multi- stakeholder governance mechanisms that currently exist with respect to different Internet issues and functions. Finally, the WGIG assessed a number of alternative definitions proposed by various parties in the course of the WSIS process and related international discussions. 10. Taking into account the criteria, analysis and proposals mentioned above, as well as the larger debate among stakeholders involved in WSIS, WGIG and the broader Internet community, the WGIG provides the following working definition: Internet governance is the development and application by Governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet. 11. This working definition reinforces the concept of inclusiveness of Governments, the private sector and civil society in the mechanisms of Internet governance. This working definition also acknowledges that with respect to specific issues of Internet governance each group will have different interests, roles and participation, which in some cases will overlap.	STAKEHOLDER COOPERATION for: coordinate/cooperate in preserving multistakeholder internet governance STAKEHOLDER COOPERATION for: establishing a standing multistakeholder engagement mechanism in order to address stability issues (this includes adequate involvement and consultation of states, non-state actors such as private sector entities, and civil society)
192:2	2005 - UN WGIG REPORT	2005	(a) Issues relating to infrastructure and the management of critical Internet resources, including administration of the domain name system and Internet protocol addresses (IP addresses), administration of the root server system, technical standards, peering and interconnection, telecommunications infrastructure, including innovative and convergent technologies, as well as multilingualization. These issues are matters of direct relevance to Internet governance and fall within the ambit of existing organizations with responsibility for these matters	CRITICAL INFRASTRUCTURE CBM: define critical infrastructure CRITICAL INFRASTRUCTURE for: promoting resilience (as related to ICTs,cybersecurity, and related critical infrastructure CRITICAL INFRASTRUCTURE for: protecting critical infrastructures
192:3	2005 - UN WGIG REPORT	2005	Freedom of expression Restrictions on freedom of expression. • Measures taken in relation to the Internet on grounds of security or to fight crime can lead to violations of the provisions for freedom of expression as contained in the Universal Declaration of Human Rights and in the WSIS Declaration of Principles	HUMAN RIGHTS for: respecting human rights and fundamental freedoms; applying them to cyber space / ICT use, etc. STATE RESPONSIBILITY for: adhering to rules and regulations agreed upon by previously enacted international law/mandates/treaties
192:4	2005 - UN WGIG REPORT	2005	(c) Issues that are relevant to the Internet but have an impact much wider than the Internet and for which existing organizations are responsible, such as intellectual property rights (IPRs) or international trade. The WGIG started examining the extent to which these matters are being handled consistent with the Declaration of Principles;	CONFIDENCE BUILDING CBM: recognize importance of ICTs as the key driver of governance, economy, commerce, trade, and social well-being DIGITAL ECONOMY CBM: recognize the importance of the relationship between trade and the digital economy
192:5	2005 - UN WGIG REPORT	2005	Combating cybercrime.	STAKEHOLDER COOPERATION for: coordinate/cooperate in combatting cybercrime
192:6	2005 - UN WGIG REPORT	2005	• Fostering international and regional cooperation. • Promoting the development of infrastructure and ICT applications	CONFIDENCE BUILDING for: promote cooperation in regional confidence-building measures (CBMs) INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information NORM for: promote cooperation in training to develop ICT/cybersecurity awareness and skills
192:7	2005 - UN WGIG REPORT	2005	• Development of best practices.	INFORMATION EXCHANGE for: sharing of good/best practices in relation to ICTs and cybersecurity
192:8	2005 - UN WGIG REPORT	2005	Promoting capacity-building	CAPACITY BUILDING CBM: develop regional approaches to capacity-building CAPACITY BUILDING CBM: encourage further work in capacity-building
192:9	2005 - UN WGIG REPORT	2005	Research and development of technologies and standards.	CONFIDENCE BUILDING CBM: further investments in ICT research and development INFORMATION EXCHANGE CBM: encourage further analysis and study by research institutes and universities on ICT security related matters INFORMATION EXCHANGE CBM: encouraging exchanges between research and academic institutions

ID	Document	Document Groups	Quotation Content	Codes
192:10	2005 - UN WGIG REPORT	2005	44. The forum should preferably be linked to the United Nations, in a form to be defined. It would be better placed than existing Internet institutions to engage developing countries in a policy dialogue. This would be an important factor in itself, as the future growth of the Internet is expected to be mainly in developing countries.	UNITED NATIONS CBM: the United Nations (UN) may serve as an international body for decision-making, framework creation/implementation, and when developing and adopting universally agreed upon ICT norms/rules/principles (in order to ensure peace and responsible behavior/ICT use)
192:11	2005 - UN WGIG REPORT	2005	45. The forum should be open to all stakeholders from all countries; any stakeholder could bring up any Internet governance issue. The forum would be reinforced by regional, subregional and national initiatives and supplemented by open online mechanisms for participation. It should support the information and communication technologies for development (ICT4D) agenda emerging from the WSIS and Millennium Development Goals (MDG) processes. It could assume, inter alia, the following functions:	STAKEHOLDER COOPERATION for: coordinate/cooperate in preserving multistakeholder internet governance
192:12	2005 - UN WGIG REPORT	2005	35. The WGIG addressed the adequacy of current Internet governance arrangements in relation to the principles outlined in the final WSIS documents and came to the conclusion that some adjustments needed to be made to bring these arrangements more in line with the WSIS criteria of transparency, accountability, multilateralism and the need to address all public policy issues related to Internet governance in a coordinated manner. It grouped these issues in four clusters: a forum, global public policy and oversight, institutional coordination, and regional, subregional and national coordination.	CONFIDENCE BUILDING CBM: voluntary transparency STAKEHOLDER COOPERATION CBM: states should participate and cooperate in multilateral forums
193:1	1997 - WTO _ ITA introduction		Subscribed initially by 29 members, participation quickly increased at the beginning of 1997 when a number of other members decided to join the Agreement. Today, following the recent accession of the Republic of Seychelles, the ITA now covers 81 WTO members, which account for approximately 97 per cent of world trade in information technology products.	INFORMATION EXCHANGE for: transnational/international cooperation and exchange of information STAKEHOLDER COOPERATION CBM: states should participate and cooperate in multilateral forums