ANU College of Law
Australian National University

Canberra ACT 0200 Australia
www.law.anu.edu.au
Sarah.Heathcote@anu.edu.au
Esme.Shirlow@anu.edu.au

9 June 2020

Response to Australia's CCTIES Consultation

This submission responds to the Department of Foreign Affairs and Trade's call for submissions on **Australia's Cyber and Critical Technology International Engagement Strategy** (CCTIES).

Overview of the authors

Dr Sarah Heathcote is an Associate Professor at the ANU College of Law. She teaches and researches in the fields of public international law and the law of international organizations. Dr Heathcote worked for over a decade at the University of Geneva and for Boston University before joining the ANU in 2008.

Dr Esmé Shirlow is a Senior Lecturer at the ANU College of Law. Dr Shirlow teaches and researches in the fields of public international law, international dispute settlement, and international investment law and arbitration. Dr Shirlow currently serves as an assistant to a number of investment treaty tribunals, and also advises parties to investment treaty claims and in proceedings before the International Court of Justice. Prior to joining the ANU, she worked in the Australian Attorney-General's Office of International Law.

In 2019, the authors were involved in a funded project with the ANU Cyber Institute ('Regional Cyber Futures Scoping Study'), for which they produced a report titled 'Legal Frameworks in the Indo-Pacific Region: Cyber Resilience of Critical Infrastructure in Indonesia's Energy Sector'. This report can be provided on request.

Our response to the Department's questions follows.

What should Australia's key international cyber and critical technology objectives be? What are the values and principles Australia should promote regarding cyberspace and critical technology?

Australia – like other States – has economic, social and security interests in maintaining stable and secure cyberspaces and in protecting its critical technology. Given that cyber activities are inherently dynamic and border-crossing, the successful regulation of cyber activities cannot occur unilaterally and necessitates coordination, and where possible, cooperation with other States. To delineate and achieve its objectives in relation to cyber and critical technology, Australia should consider international regulation with the following factors in mind.

(a) *Australia's approach should be based upon coordination and/or cooperation with other States*

Cyber activities implicate the interests and authority of many States because they cross borders, can occur in the global commons - territories subject to the sovereignty of no State (such as the high seas and outer space) - or implicate the interests of multiple States even if they occur within a single State's territory. The stability, security, and protection of cyberspace is therefore best achieved in cooperation with other States.

A law of cooperation implies institutions: Cooperation and stability in respect of cyberspace and critical technology is best achieved through international institutions. This is particularly the case when the regulatory regime requires the implementation of positive obligations, as opposed to those requiring a State merely to refrain unilaterally from a particular course of action. Thus an institution is useful for developing norms encouraging States towards a certain course of action in order to achieve a result that may not be possible to achieve immediately (often phrased as 'best-efforts' obligations). So too, the sharing of best practice, or compliance monitoring with established standards, can best be achieved in an international institutional framework.

Coordination is a next best alternative: Even where institutional regulation is elusive, multilateralism for the development of rules should be pursued to achieve Australia's overarching objective of cyber regulation. While a multilateral regime lends itself to coordination of State activities and plays an important role in the development of rules, it is harder to achieve cooperative activities such as monitoring without an institution, especially when seeking to reconcile approaches between States with political differences. Thus whilst, for instance, a Conference of the Parties (COP) might be sufficient for some cooperative activity, it is a weak solution as it does not produce an entity with a legal personality distinct from the States parties to the initiative – with the benefits of impartiality, specialisation, and institutional memory that come with an independent institution, even if it is only in a simplified treaty-body form.

The nature of the cybersphere lends itself to regulation by certain types of rules (obligations): The cybersphere can be described as a global public good, insofar as a failure by one State to respect cyber regulation impacts the efficacy of the legal regime for all States. As such, the cybersphere lends itself to governance by a regime of so-called 'integral' obligations (also known as *erga omnes partes* obligations). Such obligations are those in respect of which all States have an interest in securing compliance since an act by any party to the regime will affect every other party. Climate change or a nuclear disarmament regime would be other illustrations. That said, whilst an *erga omnes partes* regime might be an ideal form of regulation for the cybersphere – usually in the form of a treaty establishing the obligations of all parties – the political climate may not, at least for the time being, allow such regulation as it depends on the existence of a heightened sense of community amongst participants. Nonetheless, because of these inherent characteristics of the cybersphere as a global public good, from an international law perspective, the pursuit where politically possible by Australia of at least a multilateral approach to cyber regulation (even if it does not legally adopt any integral characteristics), is certainly the preferred option for regulation.

Developing definitions: One key way in which Australia can seek to coordinate and achieve consensus with other States vis-à-vis its international cyber policy is through the harmonisation of key definitions relevant to legal regulation of cyberspace. Adopting common definitions minimises barriers to misunderstanding and disagreement. Developing a common lexicon to refer to international legal rules in cyberspaces would provide a platform for discussion, and ultimately further consensus on regulatory approaches. Agreement on basic terms is a critical first step to deconstructing and understanding diverse perspectives and practices towards regulation of cyberspaces. In this context it is important to acknowledge that sometimes a technical legal term such as attribution may not carry the same meaning as in other contexts. It is crucial that any such differences be identified and clarified. States like Australia have an important opportunity to structure the coverage of the definitions applicable to cyberspace. Such definitions may, in turn, influence or inform future approaches to such definitions by other States and international organizations. Developing joint definitions of key concepts will facilitate inter-State cooperation and coordination and ensure that States have a clear framework in which to develop and apply international law in this field. It is important to bear in mind that a definition developed by one State, or one group of States, does not apply to States outside that group. To take an example, the definition of 'critical infrastructure' developed by Australia with 'Five Eyes' partner New Zealand, and which includes banking and finance[1], neither binds nor is it in other respects applicable to other States, unless and to the extent that those States consent to adopt that definition for their own purposes. That said, even non-opposable definitions are nevertheless useful as templates for the development of a commonly accepted definition. Their value as starting points is also due to the fact that they represent a position accepted by at least one State or group of States. Overlap provides an existing consensus and basis from which States, including third States, can extrapolate a more universally applicable legal definition.

(a) ***Australia's approach should be rules-based***

Cyber regulation, whether through a cooperative or coordinating regime, is best achieved by pursuing a 'rules based international order'.

General or specific rules?: The majority of international rules impacting the entities, objects and spaces relevant to cyber-governance are presently rules of general application, rather than rules framed by reference to the specific characteristics or context of cyberspaces. A continuing issue for Australia is whether cyber-governance activities should take place by reference to these existing rules of general application, or whether new – more specific – rules should be developed. Specific rules have the advantage of being more readily applicable, but have the drawback of being less likely to cater to situations that have not yet been envisaged. They are also difficult to arrive at, given blockages in international negotiations on these topics (particularly at present). Australia should continue to apply international law to cyberspace, and continue its efforts to support the development of both specific and general rules of international law in that context.

Specific rules of international law: The fact that few cyber-specific international rules exist reflects the difficulties associated with reaching consensus on a comprehensive regime of international cyber law. States may be able to generate such consensus, however, where international law-making efforts are restricted to addressing specific sectors or cross-cutting cyber issues. Such consensus might, moreover, be particularly likely where States cooperate on international cyber-governance initiatives on a bilateral or regional basis. There might, for example, be particular scope to create a regional set of cyber rules (including, for instance, for the ASEAN region). Australia could alternatively seek to leverage its own capabilities, and the

[1] Australia-New Zealand Counter-Terrorism Committee 'National Guidelines for Protecting Critical Infrastructure from Terrorism', 2015, p. 3.

capacities of other States, to develop sector-specific cyber norms, including capacity-building initiatives.

Although some actors might perceive an advantage in opaque rules or claim that none apply altogether (although as will be seen, general international law will always take a position) Australia could consider spearheading the development of certain specific rules. For example: although the general international law principle of due diligence applies in cyberspace, Australia could consider whether to coordinate with other States or in international settings to develop specific due diligence rules or guidelines concerning the application of that principle in cyberspace or in respect of particular sectors. Such clarifications might address, for instance, what standard will be considered sufficient to discharge a due diligence obligation. This might entail clarifying whether a State is obligated to take 'appropriate', 'proportionate', or 'reasonable' measures, or otherwise 'all measures that are feasible in the circumstances'.[2] In addition, Australia could clarify what standard of foreseeability or knowledge should apply. Due diligence obligations will differ, for instance, depending upon whether they are interpreted to require a State to respond to harms that it *knows* are emanating from its territory, or rather whether the harm must only be *foreseeable*, either subjectively to the State or objectively on the facts. A due diligence obligation might otherwise be developed to entail an obligation of active monitoring in cyber spaces. Finally, due diligence obligations could be further refined to define the threshold at which harm to another State will trigger the application of the due diligence obligation. This might be, for instance, 'serious adverse consequences',[3] or some other threshold of harm.

Specific principles on cyber due diligence could be developed in one of two ways. First, States could conclude a treaty to this effect, undertaking obligations of due diligence with respect to particular cyber activities on their territories. Alternatively, a due diligence standard might crystallise under customary international law, insofar as States adopt domestic laws and practices in purported application in cyberspaces of their general due diligence obligations under international law. As will be seen under the next heading, this definition might be progressively nudged forward through the adoption of international political instruments such as guidelines or non-binding resolutions. The development of a due diligence obligation applicable to cyberspace is likely to be a key priority for future regulation given that many cyber incidents are initiated by non-State actors, and in light of the difficulties of legal and factual attribution associated with cyber conduct.

Legal techniques for developing specific rules of international law for cyberspace: Rules encapsulated in sources of international law like treaties have the advantage of binding States or non-State entities to particular courses of conduct, rather than merely encouraging them to act in a particular way. The development of treaties, however, may be particularly difficult where States do not wish to make binding concessions that will constrain their future conduct. The use of treaties in cyber law-making also risks fracturing governance structures and norms. This is because States are particularly unlikely to agree to cyber-norms on a multilateral basis given the plethora of views likely to be represented in multilateral fora. As such, smaller groups of like-minded States may achieve better results. Such fragmented law-making risks, however, the generation of overlapping and conflicting cyber-governance regimes. It is therefore vital for each State to closely monitor how cyber law-making efforts by both itself and its treaty

[2] Michael N. Schmitt and NATO Cooperative Cyber Defence Centre of Excellence, 'Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations' (2017, Cambridge University Press), Rule 7.
[3] Michael N. Schmitt and NATO Cooperative Cyber Defence Centre of Excellence, 'Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations' (2017, Cambridge University Press), Rule 6.

partners correlate to its existing international and domestic legal frameworks. Reaching agreement in treaties may also require States to obscure a lack of consensus by watered down or vague rules. This risks making the outputs of treaty law-making processes particularly difficult to apply.

The development of customary international law is not constrained by this difficulty because it is generated through State practice and *opinio juris* (conviction that a State practice is binding) and so relies upon a latent consensus: one that need not be written down and expressly agreed by States. Due to its organic nature, however, customary international law rules relevant to cyber-regulation may be unclear and difficult to identify. This indeterminacy may generate disagreements as to the existence, content, or interpretation of customary international law where it is invoked by States. It may, furthermore, be particularly difficult to establish the requisite amount of State practice and *opinio juris* in respect of cyber norms, particularly as many State responses to such conduct will take place opaquely or otherwise be couched in political – rather than legal – terms.

One means of accommodating differences is to adopt framework agreements, whether in conventions (treaties) or in instruments of less than treaty status (for example political declarations or resolutions). Such agreements would allow States to subscribe to specific differentiated obligations tailored for instance to their own levels of development but under a common umbrella principle. A number of treaties of this sort exist internationally such as the Framework Convention on Tobacco Control. Such instruments could be binding (as treaties), or non-binding guidelines (soft law), and could be universal or regional. Political arrangements may be both easier to develop and easier to amend. They also have the advantage of potentially encompassing non-State actors who themselves are not able to make treaties or generate customary international law. Such flexibilities also apply, however, at the point of compliance. States retain significant discretion to disregard political arrangements, and they may thus be less able than treaties to generate compliance where it matters most.

Australia could balance the strengths and weaknesses of these legal techniques by sequencing its approach to generating rules on cyber conduct, beginning with softer norms in political agreements but with an ultimate view to securing harder law-making after key actors become socialised towards a particular regulatory approach.

Another means of establishing consensus in a difficult political environment is by identifying existing positions under domestic law. If there is a lack of political will to reach agreement on cyber specific governance, an important role Australia could play in order to secure common definitions is to undertake a forensic study of the domestic legislation of the world's States in order to identify inductively the common understanding that States have in their domestic legal orders of, for instance, critical infrastructure and its interaction with cyber. In other words, a point of consensus no doubt currently exists globally, it is just that it is not yet known.

General rules of international law: If for political reasons specific rules cannot be developed, the reach of existing general rules should not be underestimated. There are no gaps in international law – it always has something to say in relation to the legality of a particular situation or event. So, for instance, if a cyber-attack results in the loss of power to a hospital then even in the absence of a rule envisaging that precise scenario law can be applied to determine the consequences of the act. If there is an armed conflict within the meaning of the law, international humanitarian law will apply, and if such an attack occurs outside of an armed conflict, international human rights law will apply. Moreover, the criminal law of the State on whose territory the attack takes place also applies. A State's laws can (if sometimes controversially) also apply when the victim of the attack is a national of the State seeking to apply its laws. There is in sum, no shortage of applicable law but (1) its identification and (2) proof of its application to a particular situation – generally a question of establishing fact not law – can present difficulties. Tallinn Manual 2.0 does a good job in regard to the identification of general rules. The difficulty is that it represents one perspective, drafted by a pro-NATO group of jurists. Australia could therefore usefully take specific steps to engage other types of States, at all levels, with a view to clarifying how general rules of international law apply in cyberspace.

Countering the retreat from an open global cybersphere: Regardless of the forum or level of engagement, for a middle power such as Australia, international law and its development are particularly important. This remains the case despite current attempts by some States to privatise or bifurcate the internet, in order to carve out a separate cyberspace for their nationals. Not only does law provide certainty and so enhance security, general international law (including for example international human rights law) will continue to bind those States that seek to privatise a cybersphere, making a complete legal opt-out impossible. Partly for this reason all serious norm developing initiatives are welcome. This is the case whether it is with Australia's traditional allies or others. Australia should always be open to dialogue with those with whom it disagrees or has diverging views. Whilst existing codification attempts including the Tallinn Manual 2.0 need to be welcomed in general and, where Australia agrees with the principles set out, applauded, we must also recognise their (Western) provenance and encourage others to put forward their views and engage on them. It is very important that Australia does not end up subscribing to siloed positions on the law. The law will lose much of its relevance if only friends agree. Initiatives to promote the codification of applicable general and specific cyber-related law at the multilateral level including by non-State entities such as academics or other eminent jurists (for instance the International Law Commission, a subsidiary body of the United Nations General Assembly) are a means of being both objective and inclusive.

(b) Australia should focus on both normative and operational aspects of cyber governance

Cyber initiatives differ in focus, depending upon whether they are concerned with normative or operational activities. It is fair to say that many international institutions today engage in both types of activity even if they were initially only established to deal with one alone, illustrating the difficulty in keeping these types of activity completely separate. 'Normative' activities include the development and adoption of rules to govern cyber activities, including in the form of laws, standards or guidelines. 'Operational' activities include performing monitoring and compliance duties, exercising dispute settlement functions, or issuing emergency warnings.

It would seem that, partly as a function of the international political climate, Australia has so far focussed predominantly upon developing operational rather than normative functions in cyberspace, and it has done so with a particular focus on resilience. Such initiatives are important to support capacity building internationally, including within the Indo-Pacific region, both for States actors and actors in the private sector. Australia could further support capacity to respond to cyber incidents by establishing agencies or organizations to perform cross-sectoral operational activities including, for instance, security threat evaluations; the issuing of security alerts; or the auditing of systems for cyber reliability and/or vulnerability.

Australia's normative activities have so far been more limited. At the multilateral level this includes, principally, a focus upon engagement in the UNGGE process, although Australia's normative engagement otherwise appear to have been as a relatively passive adopter of normative frameworks established by some of its politically and strategically aligned partners, such as the (albeit academic) NATO Cooperative Cyber Defence Centre of Excellence's Tallinn Manual 2.0. on the International Law Applicable to Cyber Operations. We also understand that Australia is engaged regionally with ASEAN and bilaterally with a number of partners and that these initiatives can include a normative content. All such efforts should be encouraged.

(c) Australia should pursue multi-stakeholder initiatives

Australia should wherever possible pursue a multi-stakeholder model for cyber regulation, incorporating private (non-State) actors in regulatory efforts. The involvement of non-State actors in cyber-regulation reflects a recognition that such actors are often the principal players and threats in cyberspaces. States thus have much to gain from the engagement of these actors in their cyber-governance activities. A key benefit of incorporating non-State actor participation in cyber-governance activities is that such actors will typically have specialised expertise relevant to the topics to be regulated. They may, moreover, be the principal threats to the sector in question, such that States may wish to involve them in norm-generation or enforcement processes in order to encourage their compliance with resulting governance outputs.

To pursue a multi-stakeholder approach, Australia must seek to ensure that stakeholders in cyberspace can not only master the law but also participate effectively in its development and implementation. Further capacity building in this respect could take the form of guidelines produced by State/s or international organizations to equip private sector stakeholders as well as government entities to better respond to cyber incidents. Cyber guidelines could address, *inter alia*, information sharing practices amongst stakeholders; the role of industry and the State in respect of cybersecurity; and how to respond to cyber incidents. Such guidelines could be accompanied by training or guidance on relevant reporting and compliance obligations under domestic and international legal frameworks, including those that address cyber incidents implicating critical infrastructure. Guidelines for responding to cyber incidents have already been produced by some States (a normative activity) and may serve as a basis for the development of guidelines by other States or international organizations. The US Department of Justice, for instance, has developed 'Best Practices for Victim Response and Reporting of Cyber Incidents, Version 2.0' (2018). States and international organizations might alternatively draw upon analogies to other fields of law in considering how to equip stakeholders to respond to cyber incidents including, for example, disaster response and relief law and/or environmental law.

(d) Australia should work towards bolstering cyber supervision mechanisms

Monitoring mechanisms can be useful tools for impartial fact finding and the consequent diffusion of disagreement. One area where such tools might be particularly useful is in relation to attribution. To respond to the difficulties associated with both factual and legal attribution in cyberspaces an international attribution mechanism would create greater certainty and trust. Such a mechanism may adopt a range of differing structures and mandates. It could conceivably have normative capabilities in addition to its operational ones. It could, for instance, be created to develop principles of attribution applicable to cyber incidents. It could otherwise be established as an early response or dispute settlement mechanism. The members of such a mechanism could be drawn from neutral parties, and could be ‘mixed’ in nature, meaning that it would bring together private as well as government actors.

How will cyberspace and critical technology shape the international strategic/geopolitical environment out to 2030?

Regardless of the technological changes that occur going forward, it is important to stress that the rules of international law will necessarily remain applicable to the cybersphere, as detailed above. Some might need adaptation and for this reason, it is important that institutions or looser channels exist in which States and other actors can engage in normative and operational activities. A number of international institutions already exist that deal in one way or the other with the cybersphere and these are annexed to this document. The list does not purport to be exhaustive.

How should Australia pursue our cyber and critical technology interests internationally?

Please see above.

How can government, industry, civil society and academia cooperate to achieve Australia's international cyber and critical technology interests?

Both domestic and international frameworks for data collection, communication and cooperation should be created.

Public service departments should build and expand practitioners or scholars in-residence programs to achieve closer collaboration and wider engagement and input in the generation of cyber policy. More frequent policy roundtables and targeted consultation processes should also be organised to engage relevant stakeholders.

Government and academia could further collaborate to produce studies and databases collating best practice, and/or instances of State and international organisational practice vis-à-vis cyber regulation.

Internationally, as discussed above, opportunities for lines of communication to be kept open to ensure dialogue and cooperation between States as well as other stakeholders should be promoted.

More inter-disciplinary scholarship and education should also be a priority.

Appendix: International Cyber Governance Entities (as at December 2018)

The below list introduces key international governmental and non-governmental entities which have sought to address issues of cyber-governance at the international level. The list provides details of the entities and details of the cyber initiatives developed by these entities which are relevant to the regulation of cyber opportunities and challenges. The list is organised alphabetically. Some of the entities listed are international organizations with a legal personality distinct from their members and others are looser institutional arrangements. Purely domestic organizations are not included.

Entity/Initiative	Structure	Background	Connections to Other Stakeholders on Cyber	Key Outputs Relevant to Cyber-Governance
African Union ('AU')	Intergovernmental	The AU was established in 2002 (replacing the 'Organization of African Unity, which was established in 1963). The AU is an intergovernmental organization comprising 55 African States.[4]	The AU has collaborated with the Council of Europe on cybersecurity matters.[5] Huawei has also provided training to AU officials under a MOU signed by the AU and Huawei (2015).[6] In 2017, the AU Commission produced Guidelines in collaboration with a non-governmental organization (the Internet Society[7]), by which it was resolved to form 'an Africa-wide Cyber Security Collaboration and Coordination', which was envisaged as 'a multistakeholder group that would advise policymakers of the AC on regional strategies and capacity building, and facilitate	• Declaration on Internet Governance (2017)[10] • Internet Infrastructure Security Guidelines for Africa (A Joint Initiative of the Internet Society and the Commission of the African Union) (2017)[11] • Final Communique of the First Extraordinary Session of the Specialized Technical Committee on Communication and Information and Communication Technology (2016)[12] • African Union Convention on Cyber Security and Personal Data Protection (2014)[13] • Draft African Union Convention on the Establishment of a Credible Legal Framework for Cyber Security in Africa (2012)[14] • Khartoum Declaration (2012)[15]

[4] Algeria, Angola, Benin, Botswana, Burkina Faso, Burundi, Cameroon, Cabo Verde, Central African Republic, Chad, Comoros, Congo, the Democratic Republic of Congo, Cote d'Ivoire, Djibouti, Equatorial Guinea, Egypt, Eritrea, Ethiopia, Gabon, Gambia, Ghana, Guinea, Guinea-Bissau. Kenya, the Kingdom of Lesotho, Liberia, Libya, Madagascar, Malawi, Mali, Mauritania, Mauritius, Morocco, Mozambique, Namibia, Niger, Nigeria, Rwanda, Saharawi Arab Democratic Republic, Sao Tome and Principe, Senegal, Seychelles, Sierra Leone, Somalia, South Africa, South Sudan, Sudan, Kingdom of Swaziland, Tanzania, Togo, Tunisia, Uganda, Zambia and Zimbabwe.

[5] See, for example,: AU, 'African Union Commission and Council of Europe Join Forces on Cybersecurity' (12 April 2018) <https://au.int/en/pressreleases/20180412/african-union-commission-and-council-europe-join-forces-cybersecurity>.

[6] <https://au.int/en/pressreleases/20151203-3>

[7] <https://www.internetsociety.org/about-internet-society/>

[10] <https://au.int/sites/.../33025-rp-declaration_on_internet_governance-english.docx>

[11] <https://www.internetsociety.org/resources/doc/2017/internet-infrastructure-security-guidelines-for-africa/>

[12] <https://au.int/en/pressreleases/20160916>

[13] *African Union Convention on Cyber Security and Personal Data Protection* <https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection> (drafted 2011, adopted 2014, but yet to enter into force)

[14] <https://au.int/en/cyberlegislation>

[15]<https://au.int/sites/default/files/newsevents/pressreleases/27218-pr-declaration_khartoum_citmc4_eng_final_0.pdf>

Entity/Initiative	Structure	Background	Connections to Other Stakeholders on Cyber	Key Outputs Relevant to Cyber-Governance
			information sharing across the region'.[8] In 2018, the AU Commission organised an 'African Forum on Cybercrime' which was supported by the Council of Europe, the European Union, INTERPOL, UNODC, the US, the UK, and the Commonwealth Secretariat (with participation of a range of other international organizations).[9]	
Asia-Pacific Economic Cooperation ('APEC')	Intergovernmental	APEC was established in 1989 and comprises 21 member States.[16] APEC has addressed cyber issues through ministerial level meetings and meetings of a 'Telecommunications and Information Working Group'.[17] The Working Group comprises a series of steering groups: a Liberalisation Steering Group; an ICT Development Steering Group; and a Security and Prosperity Steering Group.[18]		• APEC Cyber Security Strategy (2002)[19] • Shanghai Declaration, from the Fifth APEC Ministerial Meeting on the Telecommunications and Information Industry (2002)[20] • Lima Declaration, from the Sixth APEC Ministerial Meeting on the Telecommunications and Information Industry (2005)[21] • APEC Strategy to Ensure a Trusted, Secure and Sustainable Online Environment (2005)[22] • APEC Telecommunications and Information Working Group Strategic Action Plan 2010-2015 (2010)[23] • APEC Telecommunications and Information Working Group Strategic Action Plan 2016-2020 (2015)[24]
Asia-Pacific Telecommunity ('APT')	Multi-stakeholder	APT was established in 1979, and comprises 38 State members (including Indonesia), 4 associate	APT was jointly established by the United Nations Economic and Social	APT holds an annual cybersecurity forum designed 'to bring together stakeholders responsible for cybersecurity systems in the Asia-Pacific region to enhance the

[8] <https://www.internetsociety.org/resources/doc/2017/internet-infrastructure-security-guidelines-for-africa/>

[9] <https://au.int/en/newsevents/20181016/first-african-forum-cybercrime>

[16] Australia, Brunei Darussalam, Canada, Chile, China, Hong Kong, Indonesia, Japan, Republic of Korea, Malaysia, Mexico, New Zealand, Papua New Guinea, Peru, The Philippines, Russia, Singapore, Chinese Taipei, Thailand, US, Vietnam.

[17] See, further: <https://www.apec.org/Groups/SOM-Steering-Committee-on-Economic-and-Technical-Cooperation/Working-Groups/Telecommunications-and-Information>

[18] See generally: <https://www.apec.org/Groups/SOM-Steering-Committee-on-Economic-and-Technical-Cooperation/Working-Groups/Telecommunications-and-Information>

[19] <https://ccdcoe.org/sites/default/files/documents/APEC-020823-CyberSecurityStrategy.pdf>

[20] <www.apec.org/~/media/Files/MinisterialStatements/.../02_telmm_001.pdf>

[21] <https://www.apec.org/Meeting-Papers/Annual-Ministerial-Meetings/2005/2005_amm>

[22] <https://www.apec.org/-/media/Files/Groups/TEL/05_TEL_APECStrategy.pdf>

[23] <https://www.apec.org/Meeting-Papers/Sectoral-Ministerial-Meetings/Telecommunications-and-Information/2010_tel/ActionPlan>

[24] <https://www.apec.org/Groups/SOM-Steering-Committee-on-Economic-and-Technical-Cooperation/Working-Groups/Telecommunications-and-Information>

Entity/Initiative	Structure	Background	Connections to Other Stakeholders on Cyber	Key Outputs Relevant to Cyber-Governance
		members, and 137 affiliate members.[25]	Commission for Asia and the Pacific, and the International Telecommunication Union.	regions collaborative efforts in combating cybercrime, enhancing cybersecurity, and countering spam activities'.[26]
Association of Southeast Asian Nations ('ASEAN')	Intergovernmental	ASEAN was established in 1967, and comprises 10 member States.[27]	In 2005 ASEAN and China issued the 'Beijing Declaration on ASEAN-China ICT Cooperative Partnership for Common Development'.[28] In 2012, they adopted a 'Plan of Action to Implement the Beijing Declaration on ASEAN-China ICT Cooperative Partnership for Common Development'.[29]	• Vientiane Action Programme 2004-2010 (2004)[30] • ASEAN Economic Community Blueprint (2008)[31] • ASEAN ICT Masterplan 2015 – 'We're Stronger When We're Connected' (2011)[32] • ASEAN Regional Forum, Statement by the Ministers of Foreign Affairs on Cooperation in Ensuring Cyber Security (2012)[33] • ASEAN Cyber Capacity Programme (2016)[34]
China-US Joint Liaison Group on Law Enforcement Cooperation	Bilateral	The Joint Liaison Group was established in 1998, and is designed to coordinate communications on law enforcement cooperation between the US and China.		The Joint Liaison Group has held a number of bilateral sessions to address a range of issues, including cybercrime.[35]
Commission on Science and Technology for Development				• 'Mapping of International Internet Public Policy Issues' (2015)[36]
Commonwealth of Nations	Intergovernmental	The Commonwealth of Nations was founded in	The Commonwealth has convened a number of ICT Ministers Forums to discuss cyber issues, in partnership with the	• Model Law on Computer and Computer Related Crime (2002, under review from 2017)[38]

[25] See, for a list of State members: https://www.apt.int/aptmembers

[26] <https://www.apt.int/2010-CSF>

[27] Brunei Darussalam, Cambodia, Indonesia, Laos, Malaysia, Myanmar, The Philippines, Singapore, Thailand and Vietnam.

[28] <https://asean.org/beijing-declaration-on-asean-china-ict-cooperative-partnership-for-common-development-beijing/>

[29] <https://asean.org/?static_post=plan-of-action-to-implement-the-beijing-declaration-on-asean-china-ict-cooperative-partnership-for-common-development-2>

[30] <https://www.asean.org/uploads/archive/VAP-10th%20ASEAN%20Summit.pdf>

[31] <https://www.asean.org/storage/images/archive/21083.pdf>

[32] <https://asean.org/?static_post=asean-ict-masterplan-2015>

[33] <http://aseanregionalforum.asean.org/files/library/ARF%20Chairman's%20Statements%20and%20Reports/The%20Nineteenth%20ASEAN%20Regional%20Forum,%202011-2012/ARF%20Statement%20on%20Cooperation%20in%20Ensuring%20Cyber%20Security.pdf>

[34] <https://www.mci.gov.sg/pressroom/news-and-stories/pressroom/2018/9/opening-remarks-by-mr-s-iswaran-at-the-asean-ministerial-conference-on-cybersecurity>

[35] See, for example: <https://www.fmprc.gov.cn/mfa_eng/wjb_663304/zzjg_663340/bmdyzs_664814/xwlb_664816/t1418659.shtml> (2016)

[36] https://unctad.org/meetings/en/SessionalDocuments/ecn162015crp2_en.pdf

[38] <http://thecommonwealth.org/sites/default/files/key_reform_pdfs/P15370_11_ROL_Model_Law_Computer_Related_Crime.pdf>

Entity/Initiative	Structure	Background	Connections to Other Stakeholders on Cyber	Key Outputs Relevant to Cyber-Governance
		1926, and comprises 53 member States.[37]	Commonwealth Telecommunications Organisation and the International Telecommunication Union.	• Commonwealth Cyber Declaration (2018)[39] • Commonwealth Heads of Government Meeting Communique, 'Towards a Common Future' (2018)[40]
Commonwealth Telecommunications Organisation ('CTO')	Multi-stakeholder	The CTO comprises 37 State Members, along with affiliate State members, ICT sector members and academia members.[41]	With the Commonwealth of Nations and ITU, the CTO convenes ICT Ministers Forums to support discussion of cyber issues amongst Commonwealth States.	• The CTO coordinates a 'Commonwealth Internet Governance Forum' which aims to support capacity building amongst Commonwealth members, and promote multi-stakeholder internet governance and cybercrime regulation.[42] • Strategic Plan of the Commonwealth Telecommunications Organisation for the Period 2016-2020 (2016)[43] • Commonwealth Cybergovernance Model (2014)[44]
Comprehensive and Progressive Agreement for Trans-Pacific Partnership ('CPTPP')	Treaty	The CPTPP will enter into force at the end of 2018, and currently comprises 11 member States.[45] Seven other States have indicated they may be interested in joining the agreement in the future (the UK, the US, Colombia, Indonesia, Republic of Korea, Taiwan, Thailand).		• Vietnam and New Zealand have concluded a side agreement related to cybersecurity, indicating their intention to 'continue consultation on cooperation for the implementation of the Cyber Security Law of Viet Nam or related legislation concerning cyber security with a view to ensuring consistency with the Agreement'.[46]
Cooperation Council for the Arab States of the Gulf / Gulf Cooperation Council ('GCC')	Intergovernmental	The GCC is an intergovernmental institution comprising six Gulf States.[47] It was established by treaty in 1981.[48]	The GCC is a member of the Financial Action Taskforce ('FATF').	• Conference hosted by the UAE, to assist GCC States to enact domestic cybercrime legislation (2007)[49] • Convention on Combating Information Technology Offences (2010)
Cooperative Cyber Defence Centre of Excellence International Group of Experts ('NATO	Expert group	The NATO Cyber Defence Centre was established in 2008 under a Memorandum of Understanding between Estonia, Germany, Italy,	The NATO Cyber Defence Centre was accredited by the North Atlantic Council of NATO as an	• Tallinn Manual on the International Law Applicable to Cyber Warfare (2013)[51] • NATO 'Cyber Defence Pledge' (2016)[52]

[37] For a list of member States see: http://thecommonwealth.org/member-countries

[39] http://thecommonwealth.org/sites/default/files/inline/CommonwealthCyberDeclaration_1.pdf

[40] http://thecommonwealth.org/sites/default/files/inline/CHOGM_2018_Communique.pdf

[41] See further: <https://cto.int/membership/>

[42] <https://cto.int/strategic-goals/cybersecurity/commonwealth-internet-governance-forum/>

[43] https://cto.int/about-the-cto/our-organisation/strategic-plan/

[44] https://cto.int/media/pr-re/Commonwealth%20Cybergovernance%20Model.pdf

[45] Australia, Brunei, Canada, Chile, Japan, Malaysia, Mexico, New Zealand, Peru, Singapore, Vietnam.

[46] https://www.mfat.govt.nz/assets/CPTPP/Viet-Nam-New-Zealand-Cyber-Security.pdf

[47] Saudi Arabia, Kuwait, Bahrain, Qatar, United Arab Emirates, Oman. See, generally: <http://www.gcc-sg.org/en-us/Pages/default.aspx>

[48] <http://www.gcc-sg.org/en-us/AboutGCC/Pages/Primarylaw.aspx>

[49] See, Ali Obaid Sultan Alkaabi, 'Combating Computer Crime: An International Perspective' (QUT PhD Thesis, 2010), p. 35.

[51] http://csef.ru/media/articles/3990/3990.pdf

[52] https://www.nato.int/cps/en/natohq/official_texts_133177.htm

Entity/Initiative	Structure	Background	Connections to Other Stakeholders on Cyber	Key Outputs Relevant to Cyber-Governance
Cyber Defence Centre')		Latvia, Lithuania, the Slovak Republic, and Spain.	International Military Organization on 28 October 2008.[50]	- Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (2017)[53]
Council of Europe ('CoE')	Intergovernmental	The CoE was established in 1949 and comprises 47 member States.[54] Six Sates (Canada, the Holy See, Israel, Japan, Mexico and the US) have been granted observer status.	The CoE's Convention on Cybercrime establishes a Cybercrime Convention Committee which is responsible for overseeing States Parties' implementation of the Convention.	- Convention on Cybercrime (2001)[55] - Additional Protocol to the Convention on Cybercrime, Concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed Through Computer Systems (2003)[56] - Terms of Reference for the Preparation of a Draft Second Additional Protocol to the Convention on Cybercrime (2017)[57]
Economic Community of West African States ('ECOWAS')	Intergovernmental	ECOWAS was established in 1975, and comprises 15 member States.[58]	ECOWAS has cooperated with the CoE to organise events related to cybercrime, including efforts to consider the harmonisation of cybercrime legislation with human rights and rule of law safeguards.[59]	- Directive 1/08/11 on Fighting Cyber Crime within ECOWAS (2011)[60] - Supplementary Act A/SA.1/01/10 on Personal Data Protection within ECOWAS (2010)[61]
Energy Charter Treaty ('ECT')	Treaty	The ECT is a treaty designed to strengthen the rule of law to support energy security and to mitigate energy-related investment and trade risks. The Energy Charter Conference has convened an Industry Advisory Panel for consultations, including in relation to cybersecurity risks.[62]	In 2014, the Energy Charter Secretariat held an expert workshop in cooperation with the OSCE to share best practices to protect energy networks from disruptions.[63]	
Energy Institute	Sector-led	The Energy Institute is a professional membership body which operates to		The Energy Institute produces a number of publications available for members,

[50] See, further: CCDCOE, 'History' <https://ccdcoe.org/history.html>.

[53] https://ccdcoe.org/tallinn-manual-20-international-law-applicable-cyber-operations-be-launched.html

[54] See, for a list of members: <https://www.coe.int/en/web/about-us/our-member-states>

[55] https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

[56] https://rm.coe.int/168008160f

[57] https://rm.coe.int/terms-of-reference-for-the-preparation-of-a-draft-2nd-additional-proto/168072362b

[58] Benin, Burkina Faso, Cape Verde, Gambia, Ghana, Guinea, Guinea-Bissau, Ivory Coast, Liberia, Mali, Niger, Nigeria, Senegal, Sierra Leone and Togo.

[59] See: http://www.ecowas.int/ecowas-and-the-council-of-europe-join-forces-to-help-west-african-countries-in-the-fight-against-cybercrime/

[60] http://www.tit.comm.ecowas.int/wp-content/uploads/2015/11/SIGNED_Cybercrime_En.pdf

[61] http://www.statewatch.org/news/2013/mar/ecowas-dp-act.pdf

[62] https://energycharter.org/media/news/article/industry-advisory-panel-holds-its-last-session-of-2018-in-bucharest/?tx_news_pi1%5Bcontroller%5D=News&tx_news_pi1%5Baction%5D=detail&cHash=eb10fff7ac0fa0de7a20593dbe9e6232

[63] https://energycharter.org/what-we-do/events/bratislava-energy-charter-forum-10-october-2014/

Entity/Initiative	Structure	Background	Connections to Other Stakeholders on Cyber	Key Outputs Relevant to Cyber-Governance
		bring together global energy experts.[64]		including some related to cybersecurity and cyber risks in the energy sector.[65]
European Union ('EU')	Intergovernmental	The EU comprises 28 member States.[66] It has regulated cyber issues through a number of organs and agencies, including the European Commission; the EU Agency for Network and Information Security; the EU Permanent Structured Co-operation (PESCO); the European Central Bank; and the Smart Grids Task Force (which has set up a number of specialised Expert Groups[67]).[68]	The EU and NATO adopted a 'Joint Declaration on EU-NATO Cooperation' in 2018 which addressed, *inter alia*, information sharing in relation to cyber-attacks.[69] The European Commission is a member of the FATF.	• Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (1995)[70] • Network and Information Security: Proposal for A European Policy Approach (2001)[71] • European Parliament Resolution on the Existence of a Global System for the Interception of Private and Commercial Communications (2001)[72] • Council Resolution on a Common Approach and Specific Actions in the Area of Network and Information Security (2002)[73] • Directive 2002/21/EC of the European Parliament and Council of 7 March 2002 on a Common Regulatory Framework for Electronic Communications Networks and Services (2002)[74] • Directive 2002/58/EC of the European Parliament and Council concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (2002)[75] • Council Resolution on a European Approach Towards a Culture of Network and Information Security (2003)[76] • Directive 2006/24/EC of the European Parliament and Council on

[64] https://www.energyinst.org/about

[65] See, for example: https://knowledge.energyinst.org/search/record?id=84527; https://knowledge.energyinst.org/search/record?id=77393; https://knowledge.energyinst.org/search/record?id=107194

[66] For a list of member States see: https://europa.eu/european-union/about-eu/countries_en#28members

[67] See: https://ec.europa.eu/energy/en/topics/market-and-consumers/smart-grids-and-meters/smart-grids-task-force

[68] See, for example: European Central Bank, 'Cybersecurity for the financial sector' <https://www.ecb.europa.eu/paym/pol/shared/pdf/qa_cybersecurity.pdf>.

[69] https://www.nato.int/cps/en/natohq/official_texts_156626.htm

[70] https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A31995L0046

[71] http://ec.europa.eu/transparency/regdoc/index.cfm?fuseaction=list&coteId=1&year=2001&number=298&language=EN

[72] https://publications.europa.eu/en/publication-detail/-/publication/c2edc2e4-241f-4af7-bfa5-a1f59cd5ebb3/language-en

[73] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32002G0216%2802%29

[74] https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A32002L0021

[75] https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32002L0058

[76] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32003G0228%2801%29

Entity/Initiative	Structure	Background	Connections to Other Stakeholders on Cyber	Key Outputs Relevant to Cyber-Governance
				the Retention of Data Generated or Processed in Connection with the Provision of Publicly Available Electronic Communications Services or of Public Communications Networks and Amending Directive 2002/58/EC (2006)[77] • Council Resolution on a Strategy for a Secure Information Society in Europe (2007)[78] • Communication from the Commission, 'Protecting Europe from Large Scale Cyber-attacks and Disruptions: Enhancing Preparedness, Security and Resilience' (2009)[79] • Communication from the Commission, 'A Digital Agenda for Europe' (2010)[80] • Communication from the Commission on Critical Information Infrastructure Protection, 'Achievements and Next Steps: Towards Global Cyber-Security' (2011)[81] • Communication from the Commission, 'Safeguarding Privacy in a Connected World: A European Data Protection Framework for the 21st Century' (2012)[82] • Communication from the Commission, 'Tackling Crime in Our Digital Age: Establishing a European Cybercrime Centre' (2012)[83] • Communication from the Commission, 'Unleashing the Potential of Cloud Computing in Europe' (2012)[84] • Directive of the European Parliament and Council concerning Measures to Ensure a High Common Level of Network and Information Security Across the Union (2013)[85] • 'Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace' (2013)[86]

[77] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32006L0024

[78] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32007G0324%2801%29

[79] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52009DC0149

[80] https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52010DC0245R(01)

[81] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52011DC0163

[82] https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A52012DC0009

[83] https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52012DC0140

[84] https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0529:FIN:EN:PDF

[85] https://www.eumonitor.eu/9353000/1/j9vvik7m1c3gyxp/vj6ytdidv0zc

[86] https://ec.europa.eu/digital-single-market/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security

Entity/Initiative	Structure	Background	Connections to Other Stakeholders on Cyber	Key Outputs Relevant to Cyber-Governance
				• Regulation of the European Parliament and Council concerning the European Union Agency for Network and Information Security (ENISA) and Repealing Regulation (EC) No 460/2004 (2013)[87] • Directive of the European Parliament and Council on Attacks Against Information Systems and Replacing Council Framework Decision 2005/222/JHA (2013)[88] • EU Cyber Defence Policy Framework (2014)[89] • Communication from the Commission, 'The European Agenda on Security' (2015)[90] • Motion of the European Parliament on 'Human rights and technology: the impact of intrusion and surveillance systems on human rights in third countries'[91] • Joint Communication to the European Parliament and the Council: 'Joint Framework on Countering Hybrid Threats, a European Union Response' (2016)[92] • Directive of the European Parliament and Council concerning Measures for a High Common Level of Security of Network and Information Systems across the Union (2016)[93] • Smart Grids Task Force, Expert Group 2 – Cybersecurity, 'Interim Report: Recommendations for the European Commission on Implementation of a Network Code on Cybersecurity' (2017)[94] • Smart Grids Task Force, Expert Group 2 – Cybersecurity, '2nd Interim Report: Recommendations for the European Commission on Implementation of a Network Code on Cybersecurity' (2018)[95]

[87] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32013R0526&from=LT

[88] https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32013L0040

[89] www.europarl.europa.eu/meetdocs/2014_2019/documents/sede/dv/sede160315eucyberdefencepolicyframework_/sede160315eucyberdefencepolicyframework_en.pdf

[90] https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/documents/basic-documents/docs/eu_agenda_on_security_en.pdf

[91] http://www.europarl.europa.eu/sides/getDoc.do?type=REPORT&reference=A8-2015-0178&language=EN

[92] https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52016JC0018

[93] https://eur-lex.europa.eu/legal-content/EN/TXT/?toc=OJ:L:2016:194:TOC&uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG

[94] https://ec.europa.eu/energy/sites/ener/files/documents/1st_interim_report_final.pdf

[95] https://ec.europa.eu/energy/sites/ener/files/sgtf_eg2_2nd_interim_report_final.pdf

Entity/Initiative	Structure	Background	Connections to Other Stakeholders on Cyber	Key Outputs Relevant to Cyber-Governance
Financial Action Task Force (‘FATF’)	Intergovernmental	The FATF was established in 1989, to make policy in relation to money laundering, terrorist financing and ‘other related threats to the integrity of the international financial system’.[96] It comprises 36 Member States.[97]	Both the European Commission and the GCC are members of the FATF. There are also a range of regional bodies that are associate members of the FATF (e.g. the Asia-Pacific Group on Money Laundering). Indonesia is not a FATF member.	• Money Laundering & Terrorist Financing Vulnerabilities of Commercial Websites and Internet Payment Systems (2008)[98] • Guidance for a Risk-Based Approach to Prepaid Cards, Mobile Payments and Internet-Based Payment Services (2013)[99]
Global Commission on the Stability of Cyberspace	Multi-stakeholder	The Commission was created to ‘develop proposals for norms and policies to enhance international security and stability and guide responsible state and non-state behavior in cyberspace’.[100] The Commission comprises representatives of government, industry, and civil society.[101]	The Commission was initiated by the Hague Centre for Strategic Studies and the EastWest Institute. The Commission’s 2018 meeting was hosted by the United Nations Institute for Disarmament Research (UNIDIR).[102]	• ‘Norm Package Singapore’ (2018)[103]
Global Forum on Cyber Expertise	Multi-stakeholder	The Forum comprises representatives from States, international organizations, and private entities and is intended to facilitate the exchange of best practices and expertise to build cyber capacity.[104]		• Delhi Communique on a GFCE Global Agenda for Cyber Capacity Building (2017)[105]
Group of Eight (‘G8’)	Intergovernmental	The G8, now G7, comprises the G7 States (Canada, France, Germany, Italy, the UK, Japan and the US) and at the time, Russia. The G8 established a Senior Experts Group on Transnational Organised		• Principles and Action Plan to Combat High-Tech Crime (1997)[106] • Birmingham Summit: Final Communique (1998)[107] • Muskoka Declaration: Recovery and New Beginnings (2010)[108] • Deauville Declaration (2011)[109]

[96] See: http://www.fatf-gafi.org/about/

[97] See list at: http://www.fatf-gafi.org/countries/#FATF

[98] http://www.fatf-gafi.org/media/fatf/documents/reports/ML%20TF%20Vulnerabilities%20of%20Commercial%20Websites%20and%20Internet%20Payment%20Systems.pdf

[99] http://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-RBA-NPPS.pdf

[100] https://cyberstability.org/

[101] https://cyberstability.org/about/

[102] https://cyberstability.org/news/gcsc-meeting-in-geneva-hosted-by-the-united-nations-institute-for-disarmament-research-unidir/

[103] https://cyberstability.org/wp-content/uploads/2018/11/GCSC-Singapore-Norm-Package-3MB.pdf

[104] https://www.thegfce.com/

[105] https://www.thegfce.com/delhi-communique/documents/publications/2017/11/24/delhi-communique

[106] http://www.irational.org/APD/CCIPS/action.htm / http://news.bbc.co.uk/2/hi/science/nature/38671.stm

[107] https://www.mofa.go.jp/policy/economy/summit/1998/fin_comniq.html

[108] http://www.g7.utoronto.ca/summit/2010muskoka/communique.html

[109] http://www.g7.utoronto.ca/summit/2011deauville/2011-internet-en.html

Entity/Initiative	Structure	Background	Connections to Other Stakeholders on Cyber	Key Outputs Relevant to Cyber-Governance
		Crime which has a 'High-Tech Crime Subgroup'. It has also established a 24/7 point-to-point network for cooperation and assistance in cybercrime matters (which encompasses participation by non-G8 States). See now G7 below		
Group of Governmental Experts of the High Contracting Parties to the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons which may be Deemed to be Excessively Injurious or to Have Indiscriminate Effects	Intergovernmental expert group	The Group was created by the States Parties to the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May be Deemed to be Excessively Injurious or to Have Indiscriminate Effects (CCW).[110]		• Report of the 2018 session of the Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems (2018)[111]
Group of Seven ('G7')	Intergovernmental	The G7 comprises Canada, France, Germany, Italy, Japan, the United Kingdom and the United States. It serves as a forum for these States to discuss issues related to, *inter alia*, international security, economic governance, and energy policy. The G7 convened a '24/7 Cybercrime Network' in 1997, and prepared an action plan addressing cybersecurity in the same year. The Network comprises some seventy countries which have		• G7 Opportunities for Collaboration (2016)[112] • Joint Declaration by G7 ICT Ministers (Action Plan on Implementing the Charter) (2016)[113] • Charter for the Digitally Connected World (2016)[114] • G7 Principles and Actions on Cyber (2016)[115] • G7 Ise-Shima Leaders' Declaration (2016)[116] • G7 Fundamental Elements of Cybersecurity for the Financial Sector (2016)[117] • G7 Foreign Ministers' Meeting, Joint Communique (2017)[118]

[110] http://undocs.org/CCW/MSP/2017/8

[111] https://www.unog.ch/80256EDD006B8954/(httpAssets)/20092911F6495FA7C125830E003F9A5B/$file/CCW_GGE.1_2018_3_final.pdf

[112] G7, 'G7 Opportunities for Collaboration' <https://ccdcoe.org/sites/default/files/documents/G7-160430-ICTMinsOpportunities.pdf>

[113] G7, 'Joint Declaration by G7 ICT Ministers' <https://ccdcoe.org/sites/default/files/documents/G7-160430-ICTMinsJointDeclaration.pdf>.

[114] G7, 'Charter for the Digitally Connected World' <https://ccdcoe.org/sites/default/files/documents/G7-160430-ICTMinsCharter_0.pdf>.

[115] G7, 'G7 Principles and Actions on Cyber' <https://ccdcoe.org/sites/default/files/documents/G7-160527-G7PrinciplesAndActions.pdf>.

[116] G7, 'G7 Ise-Shima Leaders' Declaration, G7 Ise-Shima Summit, 26-27 May 2016' <https://ccdcoe.org/sites/default/files/documents/G7-160527-IseShimaDeclaration.pdf>.

[117] G7, 'G7 Fundamental Elements of Cybersecurity for the Financial Sector' <https://www.mof.go.jp/english/international_policy/convention/g7/g7_161011_1.pdf>.

[118] G7, 'G7 Foreign Ministers' Meeting, Luca, 10-11 April 2017, Joint Communique' <https://ccdcoe.org/sites/default/files/documents/G7-170411-FM-Joint-Communique.pdf>.

Entity/Initiative	Structure	Background	Connections to Other Stakeholders on Cyber	Key Outputs Relevant to Cyber-Governance
		designated single points of contact for cybercrime matters, which are available 24 hours per day seven days per week. The Network's primary purpose is to facilitate the preservation of data for transfer through mutual legal assistance channels. The G7 convened a 'G7 Cyber Expert Group' in 2016. The Group has prepared a number of reports on cyber, which have been adopted by ministers from G7 States.		• G7 Declaration on Responsible States Behavior in Cyberspace (2017)[119] • G7 Taormina Leaders' Communique (2017)[120] • G7 Actions for Enhancing Cybersecurity for Business (2017)[121] • G7 ICT and Industry Ministers' Declaration (2017)[122] • G7 Fundamental Elements for Effective Assessment of Cybersecurity in the Financial Sector (2017)[123] • Chair's Report of the Meeting of the G7 Ise-Shima Cyber Group (2018)[124] • G7 Foreign Ministers' Communique (2018)[125] • G7 Summit Communique (2018)[126] • G7 Fundamental Elements for Third Party Cyber Risk Management in the Financial Sector (2018)[127] • G7 Fundamental Elements for Threat-led Penetration Testing (2018)[128]
Group of Twenty-One ('G21')	Intergovernmental	The G21 is one of four informal regional groups in the UN Conference on Disarmament.[129]		• Statement of the G-21 on Prevention of An Arms Race in Outer Space (2010)[130] • Statement delivered by the Democratic People's Republic of Korea on behalf of the G-21, on the

[119] G7, 'G7 Declaration on Responsible States Behavior in Cyberspace, Lucca, 11 April 2017' <https://ccdcoe.org/sites/default/files/documents/G7-170411-LuccaDeclaration.pdf>.

[120] G7, 'G7 Taormina Leaders' Communique' <https://ccdcoe.org/sites/default/files/documents/G7-170527-Taormina-Leaders-Communique.pdf>.

[121] G7, 'G7 Actions for Enhancing Cybersecurity for Businesses' <https://ccdcoe.org/sites/default/files/documents/G7-170926-CSforBusinesses.pdf>.

[122] G7, 'G7 ICT and Industry Ministers' Declaration: Making the Next Production Revolution Inclusive, Open and Secure, Torino, 25-26 September 2017' https://ccdcoe.org/sites/default/files/documents/G7-170926-ICT_Industry_Ministers_Declaration.pdf>.

[123] G7, 'G7 Fundamental Elements for Effective Assessment of Cybersecurity in the Financial Sector' <www.g7italy.it//sites/default/files/documents/G7%20Fundamental%20Elements%20for%20Effective%20Assessment%20of%20cybersecurity%20in%20the%20financial%20sector.pdf>.

[124] https://ccdcoe.org/sites/default/files/documents/G7-180423-IseShimaChairsReport.pdf

[125] https://ccdcoe.org/sites/default/files/documents/G7-180423-FoMinCommunique.pdf

[126] https://ccdcoe.org/sites/default/files/documents/G7-180609-CharlevoixSummitCommunique.pdf

[127] G7, 'G7 Fundamental Elements for Third Party Cyber Risk Management in the Financial Sector' <https://fin.gc.ca/activty/G7/pdf/G7-cyber-risk-management-gestion-risques-cybernetiques-eng.pdf>.

[128] G7, 'G7 Fundamental Elements for Threat-led Penetration Testing' <https://fin.gc.ca/activty/G7/pdf/G7-penetration-testing-tests-penetration-eng.pdf>.

[129] For a list of members see: https://www.unog.ch/__80256ee600585943.nsf/(httpPages)/2a1de6b24c2b4aa1c1257fc400455542?OpenDocument&ExpandSection=3#_Section3

[130] http://www.reachingcriticalwill.org/images/documents/Disarmament-fora/cd/2010/statements/part2/6July_G21.pdf

Entity/Initiative	Structure	Background	Connections to Other Stakeholders on Cyber	Key Outputs Relevant to Cyber-Governance
				Prevention of an Arms Race in Outer Space (2014)[131] - Working Paper submitted by Indonesia to the Conference on Disarmament on behalf of the G-21, on the prevention of an arms race in outer space (PAROS) (2015)[132]
International Energy Agency ('IEA')	Intergovernmental	The IEA was established in 1974 and is comprised of 30 member States.[133] Its focus areas are energy security, economic development, environmental awareness and engagement worldwide.[134] From 2017, the IEA has focussed on the impact of digitalisation on the energy sector, including cyber-related disruptions to the energy sector.[135]	To be a member of the IEA, States must be members of the OECD.	- Report on Digitalization & Energy (2017)[136]
International Multilateral Partnership against Cyber Threats ('IMPACT')	Multi-stakeholder	IMPACT was established in 2008 as an alliance of States, industry partners and experts.[137]	In 2011, IMPACT signed an MOU with the ITU, by which IMPACT became 'ITU's cybersecurity executing arm', providing 'ITU's 193 Member States access to expertise, facilities and resources to effectively address cyber threats'.[138] IMPACT has also signed an MOU with the United Nations Office on Drugs and Crime (UNODC) to support UNODC in its efforts to mitigate cybercrime risks for UN Member States.[139]	
International Telecommunication Union ('ITU')	Intergovernmental	The ITU is a specialized agency of the United Nations. It was established in 1865 as the 'International Telegraph Union',	The ITU has launched various initiatives related to cyber, including the International	- International Telecommunication Regulations (2013)[144]

[131] http://www.reachingcriticalwill.org/images/documents/Disarmament-fora/cd/2014/Statements/part3/5Aug_G21.pdf

[132] https://documents-dds-ny.un.org/doc/UNDOC/GEN/G15/179/47/PDF/G1517947.pdf?OpenElement

[133] See for a list of member States: https://www.iea.org/countries/members/

[134] https://www.iea.org/about/

[135] https://www.iea.org/topics/energysecurity/resilience/

[136] https://www.iea.org/publications/freepublications/publication/DigitalizationandEnergy3.pdf

[137] http://www.impact-alliance.org/home/index.html

[138] https://www.itu.int/ITU-D/cyb/publications/2012/IMPACT/IMPACT-en.pdf

[139] https://www.itu.int/ITU-D/cyb/publications/2012/IMPACT/IMPACT-en.pdf

[144] https://www.itu.int/en/wcit-12/Pages/itrs.aspx

Entity/Initiative	Structure	Background	Connections to Other Stakeholders on Cyber	Key Outputs Relevant to Cyber-Governance
		becoming the 'International Telecommunication Union' in 1934. The ITU is responsible for, *inter alia*: maintaining and extending international cooperation between members 'for the improvement and rational use of telecommunications of all kinds'; promoting and offering technical assistance 'to developing countries in the field of telecommunications'; promoting 'the development of technical facilities and their most efficient operation with a view to improving the efficiency of telecommunication services, increasing their usefulness and making them, so far as possible, generally available to the public'; and promoting 'at the international level, the adoption of a broader approach to the issues of telecommunications in the global information economy and society, by cooperating with other world and regional intergovernmental organizations and those non-governmental organizations concerned with telecommunications'.[140]	Multilateral Partnership Against Cyber Threats[141] and the World Summit on the Information Society.[142] The International Multilateral Partnership Against Cyber Threats has established regional Cyber Security Innovation Centres including, for example, in Oman (2012).[143]	• 'Building the Information Society: a Global Challenge in the New Millennium' (2003)[145] • Geneva World Summit on the Information Society, Plan of Action (2003)[146] • Tunis Commitment,[147] and Tunis Agenda for the Information Society[148] (2005) • Recommendation ITU-T X.1205, Overview of Cybersecurity (2008)[149] • Resolution 130 of the Conference of the International Telecommunication Union, Strengthening the Role of ITU in Building Confidence and Security in the Use of Information and Communication Technologies (2010)[150] • Report of the Chairman of the High-Level Experts Group (2008)[151] • Resolution 181 of the Conference of the International Telecommunication Union, Definitions and Terminology Relating to Building Confidence and Security in the Use of Information and Communication Technologies (2010)[152] • Recommendation ITU-T X.1500, Overview of Cybersecurity Information Exchange (2011)[153] • Resolution 58 of the World Telecommunication Standardization Assembly, Encourage the Creation of National Computer Incident Response Teams, Particularly for Developing Countries (2012)[154] • Resolution 69 of the World Telecommunication Development Conference, Facilitating Creation of National Computer Incident Response Teams, Particularly for Developing Countries, and

[140] *Constitution of the International Telecommunication Union*, ATS (1994) 28 (opened for signature 22 December 1992, entered into force 1 July 1994) article 2.

[141] <http://www.impact-alliance.org/home/index.html>

[142] https://www.itu.int/net/wsis/

[143] <https://ccdcoe.org/itu-impacts-first-regional-cyber-security-centre-arab-world.html>

[145] http://repository.uneca.org/handle/10855/21199

[146] https://www.itu.int/net/wsis/docs/geneva/official/poa.html

[147] https://www.itu.int/net/wsis/docs2/tunis/off/7.html

[148] https://www.itu.int/net/wsis/docs2/tunis/off/6rev1.html

[149] https://www.itu.int/rec/T-REC-X.1205-200804-I/en

[150] https://www.itu.int/osg/csd/cybersecurity/WSIS/RESOLUTION_130.pdf

[151] https://www.itu.int/en/action/cybersecurity/Documents/gca-chairman-report.pdf

[152] https://www.itu.int/osg/csd/cybersecurity/WSIS/RESOLUTION_181.pdf

[153] https://www.itu.int/rec/T-REC-X.1500-201104-I/en

[154] https://www.itu.int/en/ITU-T/wtsa12/Documents/resolutions/Resolution%2058.pdf

Entity/Initiative	Structure	Background	Connections to Other Stakeholders on Cyber	Key Outputs Relevant to Cyber-Governance
				Cooperation between them (2014)[155] - Resolution 45 of the World Telecommunication Development Conference, Mechanisms for Enhancing Cooperation on Cybersecurity, including Countering and Combating Spam (2014)[156] - Resolution 174 of the Plenipotentiary Conference of the International Telecommunication Union, ITU's Role with Regard to International Public Policy Issues relating to the Risk of Illicit Use of Information and Communication Technologies (2014)[157] - Resolution 50 of the World Telecommunication Standardization Assembly, Cybersecurity (2016)[158] - Resolution 52 of the World Telecommunication Standardization Assembly, Countering and Combating spam (2016)[159] - Resolution 130 of the Plenipotentiary Conference of the International Telecommunication Union, Strengthening the Role of ITU in Building Confidence and Security in the Use of Information and Communication Technologies (2018)[160]
Internet Governance Forum ('IGF')	Multi-stakeholder	The IGF is a 'forum for multi-stakeholder policy dialogue' designed to discuss, *inter alia*, 'public policy issues related to key elements of Internet governance' and 'solutions to the issues arising from the use and misuse of the Internet, of particular concern to everyday users'.[161]	The IGF was convened by the UN Secretary-General under the Tunis Agenda (adopted by the World Summit on the Information Society, convened by the ITU in 2006).[162]	- IGF Chair's Summary (2018)[163] - IGF 2018 Report: Technological Innovation and Internet Governance Rules (2018)[164]
International Criminal Police Organization ('INTERPOL')	Intergovernmental	INTERPOL is an international police organization comprising 194 member States.[165]	INTERPOL has four 'Strategic Partners', as follows: Entrust Datacard Group (an	- INTERPOL Global Cybercrime Strategy (2017)[167]

[155] https://ccdcoe.org/sites/default/files/documents/ITU-141210-EncourCIRTcreat.pdf
[156] https://www.itu.int/en/ITU-D/Cybersecurity/Documents/45revDubai.pdf
[157] https://www.itu.int/en/action/internet/Documents/Resolution_174_pp14.pdf
[158] https://www.itu.int/dms_pub/itu-t/opb/res/T-RES-T.50-2016-PDF-E.pdf
[159] https://www.itu.int/dms_pub/itu-t/opb/res/T-RES-T.52-2016-PDF-E.pdf
[160] https://www.itu.int/en/ITU-D/Cybersecurity/Documents/RES_130_rev_Dubai.pdf
[161] https://www.itu.int/net/wsis/docs2/tunis/off/6rev1.html
[162] http://workspace.unpan.org/sites/Internet/Documents/UNPAN96078.pdf
[163] https://www.intgovforum.org/multilingual/index.php?q=filedepot_download/6212/1417
[164] https://www.intgovforum.org/multilingual/index.php?q=filedepot_download/6212/1417
[165] https://www.interpol.int/About-INTERPOL/Overview
[167] https://www.interpol.int/Crime-areas/Cybercrime/Cybercrime

Entity/Initiative	Structure	Background	Connections to Other Stakeholders on Cyber	Key Outputs Relevant to Cyber-Governance
		INTERPOL has created a number of regional working and expert groups with mandates of relevance to cybercrime and security, including for example, the Asia-South Pacific Working Party on IT Crime.	identity-based technology provider), IDEMIA (a company providing identity and security solutions), NEC (a company providing electronics, telecommunications products, and information technology services), and Trend Micro (a company specialising in information security).[166]	
Joint Committee of the International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC)	Non-governmental expert group	The ISO and IEC are non-governmental organizations comprising representatives of domestic standards organizations. The IEC was founded in 1906, and the ISO in 1946.	The ISO has general consultative status with the United Nations Economic and Social Council.	• ISO/IEC 27001 on security management of information systems[168] • ISO/IEC 27032 on cyber-security[169] • ISO/IEC 27033 on network security[170] • ISO/IEC 27037,[171] 27041[172] and 27042[173] on incident response and forensics • ISO/IEC 15408 on the specification, development and implementation of security products[174]
Microsoft	Company		Microsoft convenes a Cyber Security Roundtable in partnership with the Munich Security Conference, the North Atlantic Council, and Rohde&Schwarz.	• A Digital Geneva Convention to Protect Cyberspace: Microsoft Policy Papers[175] • Cybersecurity Policy Framework[176] • International Cybersecurity Norms: Reducing Conflict in an Internet-Dependent World[177] • Strengthening State Cybersecurity[178] • Advancing blockchain cybersecurity[179] • Risk Management for Cybersecurity: Security Baselines[180]

[166] https://www.interpol.int/About-INTERPOL/International-partners/Strategic-Partners
[168] https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en
[169] http://www.iso27001security.com/html/27032.html
[170] http://www.iso27001security.com/html/27033.html
[171] http://www.iso27001security.com/html/27037.html
[172] http://www.iso27001security.com/html/27041.html
[173] http://www.iso27001security.com/html/27042.html
[174] https://www.iso.org/obp/ui/#iso:std:iso-iec:15408:-1:ed-3:v2:en
[175] https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW67QH
[176] https://www.microsoft.com/en-us/cybersecurity/content-hub/Cybersecurity-Policy-Framework
[177] https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/REVroA
[178] https://www.microsoft.com/en-us/cybersecurity/content-hub/Strengthening-state-cybersecurity
[179] https://www.microsoft.com/en-us/cybersecurity/content-hub/Advancing-blockchain-cybersecurity
[180] https://www.microsoft.com/en-us/cybersecurity/content-hub/risk-management-for-cybersecurity-security-baselines

Entity/Initiative	Structure	Background	Connections to Other Stakeholders on Cyber	Key Outputs Relevant to Cyber-Governance
Munich Security Conference (MSC)	Multi-stakeholder	The MSC is a forum for discussion of international security policy and convenes an annual Conference for discussion between officials and other stakeholders, including from industry, academia, civil society and non-governmental organizations.[181] The MSC also convenes various summits, including Cyber Security Summits.[182]	The sixth Cyber Security Summit was convened with cooperation of the NATO Cooperative Cyber Defence Centre of Excellence.[183] The MSC also convenes a Cyber Security Roundtable in partnership with the North Atlantic Council, Microsoft, and Rohde&Schwarz.	• Munich Security Report (2016)[184] • Report from the MSC Cyber Security Summit in Tallinn: The Weaponization of Cyber Space (2018)[185] • Munich Security Report (2018)[186]
National Council of Information Sharing and Analysis Centers ('NCI')	Sector-led	The NCI is a sector-led group designed to foster collaboration between domestic Information Sharing and Analysis Centers.[187] It was formed in 2003, and 'comprises 24 organisations designated by their sectors as their information sharing and operational arms'.[188] The NCI provides a forum: for sharing cyber and physical threats and mitigation strategies among ISACs and with government and private sector partners during both steady-state conditions and incidents requiring cross-sector response. Sharing and coordination is accomplished through daily and weekly calls between ISAC operations centers, daily reports, requests-for-information, monthly meetings, exercises, and other activities as situations require. The NCI also organizes its own drills and exercises and participates in national exercises. [189]		• Information Sharing and Analysis Centers (ISACs) and Their Role in Critical Infrastructure Protection (2016)[190]

[181] https://www.securityconference.de/en/about/about-the-msc/

[182] https://www.securityconference.de/en/cyber-security-technology/

[183] https://www.securityconference.de/en/cyber-security-technology/

[184] https://www.securityconference.de/fileadmin/MunichSecurityReport/MunichSecurityReport_2016.pdf

[185] https://www.securityconference.de/en/news/article/the-weaponization-of-cyber-space-report-from-the-msc-cyber-security-summit-in-tallinn/

[186] https://www.securityconference.de/fileadmin/images/MSR/MSC_MunichSecurityReport_2018.pdf

[187] See, further: National Council of ISACs, 'About NCI' <https://www.nationalisacs.org/>.

[188] National Council of ISACs, 'About NCI' <https://www.nationalisacs.org/>.

[189] National Council of ISACs, 'About NCI' <https://www.nationalisacs.org/>.

[190] https://docs.wixstatic.com/ugd/416668_2e3fd9c55185490abcf2d7828abfc4ca.pdf

Entity/Initiative	Structure	Background	Connections to Other Stakeholders on Cyber	Key Outputs Relevant to Cyber-Governance
North Atlantic Treaty Organization ('NATO')	Intergovernmental	NATO was established in 1949 and comprises 29 member States.[191] The NATO organisational structure includes the 'North Atlantic Council' (the principal political decision-making body at NATO, comprised of representatives from member States) and four technical and administrative agencies: the Communications and Information Agency, the Support and Procurement Agency, the Science and Technology Organization, and the Standardization Office. NATO has recognised cyberspace as a key space for collective defence actions and training. It has established a Cyber Defence Committee, Cyber Rapid Reaction teams, a Cyberspace Operations Centre, and an Industry Cyber Partnership.[192]	NATO and the EU have concluded a Technical Agreement on cyber defence (2016).[193] The NATO Cyber Defence Centre was accredited by the North Atlantic Council of NATO as an International Military Organization on 28 October 2008.[194]	• Prague Summit Declaration (2002)[195] • Riga Summit Declaration (2006)[196] • Bucharest Summit Declaration (2008)[197] • Strasbourg/Kehl Summit Declaration (2009)[198] • 'Active Engagement, Modern Defence: Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization Adopted by Heads of State and Government at the NATO Summit in Lisbon' (2010)[199] • Lisbon Summit Declaration (2010)[200] • Chicago Summit Declaration (2012)[201] • Wales Summit Declaration (2014)[202] • Cyber Defence Pledge (2016)[203] • Warsaw Summit 'Commitment to enhance resilience' (2016)[204] • Warsaw Summit Communiqué (2016)[205] • Warsaw Summit Declaration on Transatlantic Security (2016)[206] • Brussels Declaration on Transatlantic Security and Solidarity (2018)[207]
Organisation for Economic Co-operation and	Intergovernmental	The OECD is an intergovernmental organization established in		• The Seoul Declaration for the Future of the Internet Economy (2008)[210] • Recommendation of the Council on the Protection of Critical

[191] These are: Albania, Belgium, Bulgaria, Canada, Croatia, the Czech Republic, Denmark, Estonia, France, Germany, Greece, Hungary, Iceland, Italy, Latvia, Lithuania, Luxembourg, Montenegro, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Turkey, the UK, and the US.

[192] See generally: https://www.nato.int/cps/en/natohq/topics_78170.htm?selectedLocale=en

[193] https://www.nato.int/cps/ra/natohq/official_texts_133163.htm

[194] See, further: CCDCOE, 'History' <https://ccdcoe.org/history.html>.

[195] https://www.nato.int/cps/en/natohq/official_texts_19552.htm

[196] https://www.nato.int/cps/su/natohq/official_texts_37920.htm

[197] https://www.nato.int/cps/us/natohq/official_texts_8443.htm

[198] https://www.nato.int/cps/en/natohq/news_52837.htm?mode=pressrelease

[199] https://www.nato.int/cps/en/natohq/official_texts_68580.htm

[200] https://www.nato.int/cps/em/natohq/official_texts_68828.htm

[201] https://www.nato.int/cps/en/natohq/official_texts_87593.htm?selectedLocale=en

[202] https://www.nato.int/cps/en/natohq/official_texts_112964.htm

[203] https://www.nato.int/cps/en/natohq/official_texts_133177.htm

[204] https://www.nato.int/cps/en/natohq/official_texts_133180.htm

[205] https://www.nato.int/cps/en/natohq/official_texts_133169.htm

[206] https://www.nato.int/cps/en/natohq/official_texts_133168.htm

[207] https://www.nato.int/cps/en/natohq/official_texts_156620.htm?selectedLocale=en

[210] https://www.oecd-ilibrary.org/science-and-technology/the-seoul-declaration-for-the-future-of-the-internet-economy_230445718605

Entity/Initiative	Structure	Background	Connections to Other Stakeholders on Cyber	Key Outputs Relevant to Cyber-Governance
Development ('OECD')		1961,[208] comprising 34 member States. [209] The OECD created a Global Forum on Digital Security for Prosperity as a multi-stakeholder forum for discussion of digital security risks and management.		Information Infrastructures (2008)[211] - Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy (2012)[212] - OECD Privacy Framework (2013)[213] - Recommendation of the Council on Digital Government Strategies (2014)[214] - Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity (2015)[215]
Organization for Security and Co-operation in Europe ('OSCE')	Intergovernmental	The OSCE is a regional security organization comprising 57 member States.[216] It addresses cyber issues from the perspective of 'reducing the risks of conflict between states stemming from the use of ICTs'.[217] The OSCE has pursued this objective by offering measures to 'make cyberspace more predictable and offer concrete tools and mechanisms to avoid misunderstandings, including: [a] mechanism to	The OSCE cooperates with the OAS, including in relation to cybercrime.[219]	- Ministerial Council Decision No. 3/04, 'Combating the Use of the Internet for Terrorist Purposes' (2004)[220] - Ministerial Council Decision No. 7/06, 'Countering the Use of the Internet for Terrorist Purposes' (2006)[221] - Resolution on Cyber Security and Cyber Crime (2008)[222] - Resolution on Cybercrime (2010)[223] - Resolution on the Overall Approach of the OSCE to Promoting Cybersecurity (2011)[224]

[208] Convention on the Organisation for Economic Co-operation and Development (signed 14 December 1960, entered into force 30 September 1961).

[209] Australia, Austria, Belgium, Canada, Chile. Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Israel, Italy, Japan, Korea, Latvia, Lithuania, Luxembourg, Mexico, Netherlands, New Zealand, Norway, Poland, Portugal, Slovak Republic, Slovenia, Spain, Sweden, Swizterland,Turkey, the UK, and the US.

[211] https://www.oecd.org/sti/40825404.pdf

[212] https://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf

[213] http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf

[214] http://www.oecd.org/gov/digital-government/recommendation-on-digital-government-strategies.htm

[215] http://www.oecd.org/governance/digital-security-risk-management-for-economic-and-social-prosperity-9789264245471-en.htm

[216] See, for a list: https://www.osce.org/participating-states

[217] https://www.osce.org/cyber-ict-security

[219] http://www.oas.org/en/ser/dia/institutional_relations/documents/OAS_Cooperation_with_International_Organizations.pdf

[220] https://www.osce.org/mc/42647

[221] https://www.osce.org/mc/23078

[222] https://www.oscepa.org/documents/all-documents/annual-sessions/2008-astana/declaration-7/256-2008-astana-declaration-eng/file

[223] http://www.oscepa.org/documents/all-documents/annual-sessions/2010-oslo/declaration-5/267-oslo-declaration-english/file

[224] https://www.oscepa.org/documents/all-documents/annual-sessions/2011-belgrade/declaration-4/3030-belgrade-resolutions-eng/file

Entity/Initiative	Structure	Background	Connections to Other Stakeholders on Cyber	Key Outputs Relevant to Cyber-Governance
		bring together states for consultations over potential cyber/ICT security incidents to de-escalate rising tensions; [a] platform for exchanging views, national cyber/ICT security policies and approaches to allow states to better 'read' each other's intentions in cyberspace; and [c]oncrete work items, for instance to protect ICT-enabled critical infrastructure, allowing participating States to collectively enhance cyber resilience in the OSCE region for the benefit of all.'[218]		• Resolution on Cyber Security (2013)[225] • Permanent Council Decision No. 1106, 'Initial Set of OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies' (2013)[226] • Permanent Council Decision No. 1202, 'OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies' (2016)[227] • Ministerial Council Decision No. 5/16, 'OSCE Efforts Related to Reducing the Risks of Conflict Stemming from the Use of Information and Communication Technologies' (2016)[228] • Minsk Declaration and Resolutions Adopted by the OSCE Parliamentary Assembly at the Twenty-Sixth Annual Session (2017)[229]
Organization of American States ('OAS')	Intergovernmental	The OAS was established in 1948, and comprises 35 member States.[230] The OAS established a Working Group on Cyber-crime, which held its first meeting in 1999.	The OAS has cooperation agreements encompassing cyber issues with the United Nations General Secretariat, the UNODC, the African Union Commission, the Commonwealth of Nations, the Council of Europe, INTERPOL, the OECD, and the OSCE.[231]	• Comprehensive Inter-American Strategy to Combat Threats to Cybersecurity: A Multidimensional and Multidisciplinary Approach to Creating a Culture of Cybersecurity (2004)[232] • Declaration Strengthening Cyber-Security in the Americas (2012)[233] • Report of the Inter-American Commission on Human Rights, Freedom of Expression and the Internet (2013)[234] • Recommendations of the Working Group on Cyber-crime (1999, 2003,

[218] https://www.osce.org/cyber-ict-security

[225] https://www.oscepa.org/documents/all-documents/annual-sessions/2013-istanbul/declaration/1801-istanbul-declaration-eng-1/file

[226] https://www.osce.org/pc/109168

[227] https://www.osce.org/pc/227281

[228] https://www.osce.org/cio/288086

[229] https://www.oscepa.org/documents/all-documents/annual-sessions/2017-minsk/declaration-25/3555-declaration-minsk-eng/file

[230] Antigua and Barbuda, Argentina, Barbados, Belize, Bolivia, Brazil, Canada, Chile, Colombia, Costa Rica, Cuba, Dominica, Dominican Republic, Ecuador, El Salvador, Grenada, Guatemala, Guyana, Haiti, Honduras, Jamaica, Mexico, Nicaragua, Panama, Paraguay, Peru, Saint Kitts and Nevis, Saint Lucia, Saint Vincent and the Genadines, Suriname, The Bahamas, Trinidad and Tobago, the US, Uruguay, Venezuela

[231] http://www.oas.org/en/ser/dia/institutional_relations/documents/OAS_Cooperation_with_International_Organizations.pdf

[232] https://www.state.gov/p/wha/rls/59284.htm

[233] https://ccdcoe.org/sites/default/files/documents/OAS-120307-DeclarationCSAmericas.pdf

[234] http://www.oas.org/en/iachr/expression/docs/reports/2014_04_08_internet_eng%20_web.pdf

Entity/Initiative	Structure	Background	Connections to Other Stakeholders on Cyber	Key Outputs Relevant to Cyber-Governance
				2006, 2007, 2010, 2012, 2014, 2016)[235] - Latin American and Caribbean Cyber Security Trends (2014)[236] - Inter-American Committee against Terrorism, Declaration: Protection of Critical Infrastructure from Emerging Threats (2015)[237]
Organization of the Petroleum Exporting Countries ('OPEC')	Intergovernmental	OPEC was established in 1960, and comprises 15 member States, all of which are oil-exporting developing nations.[238]		
Paris Peace Forum	Multi-stakeholder	The Paris Peace Forum is an annual event designed to encourage cooperation on global challenges. It involves representatives from States, international organizations, non-government organizations, companies, experts, religious groups etc.[239]	'[T]he Forum is organized by an NGO founded in 2018 by the Körber Foundation, the Mo Ibrahim Foundation, the Institut français des relations internationales, the Institut Montaigne, Sciences Po and the French Ministry for European and Foreign Affairs'.[240]	- Paris Call for Trust and Security in Cyberspace (2018)[241]
Regional Comprehensive Economic Partnership ('RCEP')	Treaty	The RCEP is a treaty currently under negotiation between ten ASEAN States (Brunei, Cambodia, Indonesia, Laos, Malaysia, Myanmar, the Philippines, Singapore, Thailand, Vietnam) and Australia, China, India, Japan, Republic of Korea and New Zealand.		
Shanghai Cooperation Organisation ('SCO')	Intergovernmental	The SCO was established in 2001, and comprises 8 member States.[242]	The SCO has MOUs with the Commonwealth of Independent States, ASEAN, the Collective Security Treaty Organisation, the Economic Cooperation Council, the United Nations, the UNODC,	- Agreement between the Governments of the Member States of the Shanghai Cooperation Organisation on Cooperation in the Field of International Information Security (2009)[244] - Dushanbe Declaration (2014)[245] - Tashkent Declaration of the Fifteenth Anniversary of the

[235] http://www.oas.org/juridico/english/cyber_experts.htm

[236] https://www.thegfce.com/documents/publications/2014/06/01/latin-america-and-caribbean-cyber-security-trends

[237] https://www.sites.oas.org/cyber/documents/cicte%20doc%201%20declaration%20cicte00955e04.pdf

[238] These are: Algeria, Angola, Congo, Ecuador, Equatorial Guinea, Gabon, Iran, Kuwait, Libya, Nigeria, Qatar, Saudi Arabia, United Arab Emirates, Venezuela.

[239] https://parispeaceforum.org/about/

[240] https://parispeaceforum.org/about/

[241] https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/france-and-cyber-security/article/cybersecurity-paris-call-of-12-november-2018-for-trust-and-security-in

[242] India, Kazakhstan, China, the Kyrgyz Republic, Pakistan, Russia, Tajikistan, and Uzbekistan

[244] http://cis-legislation.com/document.fwx?rgn=28340

[245] eng.sectsco.org/load/199902/

Entity/Initiative	Structure	Background	Connections to Other Stakeholders on Cyber	Key Outputs Relevant to Cyber-Governance
			the UN Economic and Social Commission for Asia and the Pacific, the Conference on Interaction and Confidence-Building Measures in Asia, and the ICRC.[243]	Shanghai Cooperation Organization (2016)[246] • Draft United Nations Convention on Cooperation in Combating Information Crimes (2018)[247] • Qingdao Declaration of the Council of Heads of State of Shanghai Cooperation (2018)[248]
Trilateral Partnership for Infrastructure Investment in the Indo-Pacific	Intergovernmental	The Trilateral Partnership is an MOU between the governments of Australia, Japan and the US which was announced in July 2018 and concluded in November 2018.[249]		The Partnership is intended 'to mobilize and support the deployment of private sector investment capital to deliver major new infrastructure projects, enhance digital connectivity and energy infrastructure, and achieve mutual development goals in the Indo-Pacific'.[250]
United Nations Conference on Disarmament	Intergovernmental	The UN Conference on Disarmament is a multilateral forum for the negotiation of arms control and disarmament treaties. It was established in 1978, and comprises 65 Member States (including Indonesia)[251]		• Report of the ad hoc Committee on Prevention of an Arms Race in Outer Space (1993)[252] • Report of the ad hoc Committee on Prevention of an Arms Race in Outer Space (1994)[253] • Basic Documents of the Conference on Disarmament related to the Prevention of an Arms Race in Outer Space - prepared by the Secretariat (2006)[254] • Reports of the seven Coordinators on the work done during the 2007 session (2007)[255] • Reports of the seven Coordinators on the work done during the 2008 session (2008)[256] • Reports of the seven coordinators submitted to the President of the Conference on the work done during the 2009 session on agenda items 1 to 7 (2009)[257]

[243] http://eng.sectsco.org/cooperation/

[246] https://ccdcoe.org/sites/default/files/documents/SCO-160624-TashkentDeclaration.pdf

[247] https://www.rusemb.org.uk/fnapr/6393

[248] *eng.sectsco.org/load/443667/*

[249] https://www.pm.gov.au/media/joint-statement-governments-australia-japan-and-united-states

[250] https://www.pm.gov.au/media/joint-statement-governments-australia-japan-and-united-states

[251] https://www.unog.ch/80256EE600585943/(httpPages)/6286395D9F8DABA380256EF70073A846?OpenDocument

[252] https://documents-dds-ny.un.org/doc/UNDOC/GEN/G93/621/48/IMG/G9362148.pdf?OpenElement

[253] https://documents-dds-ny.un.org/doc/UNDOC/GEN/G94/639/71/IMG/G9463971.pdf?OpenElement

[254] https://documents-dds-ny.un.org/doc/UNDOC/GEN/G06/616/76/PDF/G0661676.pdf?OpenElement

[255] https://documents-dds-ny.un.org/doc/UNDOC/GEN/G07/632/23/PDF/G0763223.pdf?OpenElement

[256] https://documents-dds-ny.un.org/doc/UNDOC/GEN/G08/627/78/PDF/G0862778.pdf?OpenElement

[257] https://www.unog.ch/80256EDD006B8954/(httpAssets)/26B230E4AA2B9E0AC12579CD0038ABA3/$file/1877.pdf

Entity/Initiative	Structure	Background	Connections to Other Stakeholders on Cyber	Key Outputs Relevant to Cyber-Governance
				• Reports of the coordinators on agenda items one to seven (2010)[258]
United Nations Conference on Trade and Development ('UNCTAD')	Intergovernmental	UNCTAD was created by the UN General Assembly in 1964.	UNTAD forms part of the UN Secretariat that reports to the UN General Assembly and the Economic and Social Council. It is also part of the United Nations Development Group. UNCTAD and ASEAN conducted a joint 'Review of e-commerce legislation harmonization in the Association of Southeast Asian Nations' (2013).[259] It has also established a Task Force on Cyberlaws in partnership with the East African Community.[260]	• UNCTAD Global Cyberlaw Tracker[261] • Study on Prospects for Harmonizing Cyberlegislation in Latin America[262] • Study on Prospects for Harmonizing Cyberlegislation in Central America and the Caribbean[263] • 'Harmonizing Cyberlaws and Regulations: The Experience of the East African Community' (2012).[264]
United Nations General Assembly ('UNGA')	Intergovernmental	In addition to establishing a number of specialised committees, conferences, and expert and working groups to address issues associated with cyber (see above/below), the UN GA has also issued yearly resolutions on developments in the field of information and telecommunications in the context of international security, as well as resolutions on other topics with relevance to cyber-regulation.		• GA Resolution 53/70, Developments in the Field of Information and Telecommunications in the Context of International Security (1998)[265] • GA Resolution 54/49, Developments in the Field of Information and Telecommunications in the Context of International Security (1999)[266] • GA Resolution 55/28, Developments in the Field of Information and Telecommunications in the Context of International Security (2000)[267] • GA Resolution 55/63, Combating the Criminal Misuse of Information Technologies (2000)[268] • GA Resolution 56/19, Developments in the Field of Information and Telecommunications in the Context of International Security (2001)[269]

[258] https://www.unog.ch/80256EDD006B8954/(httpAssets)/748E0C9E0A888E22C12579CD0038CD8C/$file/1899.pdf

[259] https://unctad.org/en/pages/PublicationWebflyer.aspx?publicationid=623

[260] https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-EastAfrican.aspx

[261] https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Global-Legislation.aspx

[262] https://unctad.org/en/Docs/dtlstict20091_en.pdf

[263] https://unctad.org/en/Docs/dtlstict20093_en.pdf

[264] https://unctad.org/en/pages/PublicationWebflyer.aspx?publicationid=251

[265] https://undocs.org/A/RES/53/70

[266] http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/54/49

[267] http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/55/28

[268] https://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_55_63.pdf

[269] http://undocs.org/A/RES/56/19

Entity/Initiative	Structure	Background	Connections to Other Stakeholders on Cyber	Key Outputs Relevant to Cyber-Governance
				• GA Resolution 56/121, Combating the Criminal Misuse of Information Technologies (2001)[270] • GA Resolution 56/261, 'Plans of action for the implementation of the Vienna Declaration on Crime and Justice: Meeting the Challenges of the Twenty-first Century' (2001) • GA Resolution 57/239, Creation of a Global Culture of Cybersecurity (2002)[271] • GA Resolution 57/53, Developments in the Field of Information and Telecommunications in the Context of International Security (2002)[272] • GA Resolution 58/32, Developments in the Field of Information and Telecommunications in the Context of International Security (2003)[273] • GA Resolution 58/199, Creation of a Global Culture of Cybersecurity and the Protection of Critical Information Infrastructures (2003)[274] • GA Resolution 59/61, Developments in the Field of Information and Telecommunications in the Context of International Security (2004)[275] • GA Resolution 60/45, Developments in the Field of Information and Telecommunications in the Context of International Security (2005)[276] • GA Resolution 61/54, Developments in the Field of Information and Telecommunications in the Context of International Security (2006)[277] • GA Resolution 62/17, Developments in the Field of Information and Telecommunications in the Context of International Security (2007)[278] • GA Resolution 63/37, Developments in the Field of Information and Telecommunications in the Context of International Security (2008)[279]

[270] https://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_56_121.pdf

[271] https://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_57_239.pdf

[272] http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/57/53

[273] https://undocs.org/A/RES/58/32

[274] https://undocs.org/A/RES/58/199

[275] https://gafc-vote.un.org/UNODA/vote.nsf/91a5e1195dc97a630525656f005b8adf/bcc6041dba8a652285256f2e004cafa5/$FILE/59-61.pdf

[276] http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/60/45

[277] https://gafc-vote.un.org/UNODA/vote.nsf/91a5e1195dc97a630525656f005b8adf/27d66ab2098a42618525720b005f1de0/$FILE/61-54.pdf

[278] http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/62/17

[279] https://undocs.org/A/RES/63/37

Entity/Initiative	Structure	Background	Connections to Other Stakeholders on Cyber	Key Outputs Relevant to Cyber-Governance
				• GA Resolution 64/25, Developments in the Field of Information and Telecommunications in the Context of International Security (2009)[280] • GA Resolution 64/211, Creation of a Global Culture of Cybersecurity and Taking Stock of National Efforts to Protect Critical Information Infrastructures (2009)[281] • GA Resolution 65/41, Developments in the Field of Information and Telecommunications in the Context of International Security (2010)[282] • GA Resolution 66/24, Developments in the Field of Information and Telecommunications in the Context of International Security (2011)[283] • GA Resolution 67/27, Developments in the Field of Information and Telecommunications in the Context of International Security (2012)[284] • GA Resolution 68/167, The Right to Privacy in the Digital Age (2013)[285] • GA Resolution 68/178, 'Protection of human rights and fundamental freedoms while countering terrorism' (2013)[286] • GA Resolution 68/243, Developments in the Field of Information and Telecommunications in the Context of International Security (2013)[287] • United Nations General Assembly Third Committee, 'The right to privacy in the digital age' (2014)[288] • GA Resolution 69/28, Developments in the Field of Information and Telecommunications in the Context of International Security (2014)[289] • GA Resolution 70/237, Developments in the Field of Information and Telecommunications in the Context of International Security (2015)[290]

[280] http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/64/25
[281] https://undocs.org/A/RES/64/211
[282] https://gafc-vote.un.org/UNODA/vote.nsf/91a5e1195dc97a630525656f005b8adf/e542c8d6e28887a8852577d500585814/$FILE/A%20RES%2065%2041.pdf
[283] https://undocs.org/A/RES/66/24
[284] https://undocs.org/A/RES/67/27
[285] http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/68/167
[286] http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/68/178&referer=/english/&Lang=E
[287] https://undocs.org/A/RES/68/243
[288] https://undocs.org/en/A/C.3/69/L.26/Rev.1
[289] https://undocs.org/A/RES/69/28
[290] https://undocs.org/A/RES/70/237

Entity/Initiative	Structure	Background	Connections to Other Stakeholders on Cyber	Key Outputs Relevant to Cyber-Governance
				- GA Resolution 71/27, Developments in the Field of Information and Telecommunications in the Context of International Security (2016)[291] - GA Resolution 73/27, Developments in the Field of Information and Telecommunications in the Context of International Security (2018)[292]
United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security ('UNGGE')	Intergovernmental expert group	The UNGGE was established as a 'group of governmental experts…on the basis of equitable geographical distribution'. It has been tasked with studying 'existing threats in the sphere of information security and possible cooperative measures to address them, including norms, rules or principles of responsible behaviour of States and confidence-building measures, the issues of the use of information and communications technologies in conflicts and how international law applies to the use of information and communications technologies by States'.[293]		- Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (2010)[294] - Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (2013)[295] - Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (2015)[296]
United Nations Human Rights Council (UNHCR)	Intergovernmental	The UNHCR was created in 2006 and comprises 47 States elected by the UN General Assembly.[297]		- Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (2013)[298] - Report of the Office of the United Nations High Commissioner for Human Rights: The Right to Privacy in the Digital Age (2014)[299] - Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (2015)[300]

[291] http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/71/28

[292] http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/73/27

[293] United Nations General Assembly, 'Developments in the field of information and telecommunications in the context of international security', A/RES/68/243, 27 December 2013, para. 4.

[294] https://undocs.org/A/65/201

[295] United Nations General Assembly, 'Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security: Note by the Secretary-General' (24 June 2013) A/68/98, available at <https://undocs.org/A/68/98>.

[296] United Nations General Assembly, 'Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security: Note by the Secretary-General' (22 July 2015) A/70/174, available at <https://undocs.org/A/70/174>.

[297] https://www.ohchr.org/EN/HRBodies/HRC/Pages/AboutCouncil.aspx

[298] https://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf

[299] https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf

[300] https://undocs.org/A/HRC/29/32

Entity/Initiative	Structure	Background	Connections to Other Stakeholders on Cyber	Key Outputs Relevant to Cyber-Governance
				• Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (2016)[301] • Resolution adopted by the Human Rights Council on 1 July 2016, The promotion, protection and enjoyment of human rights on the Internet (2016)[302] • Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (2017)[303] • Report of the Special Rapporteur on the right to privacy (2017)[304] • Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (2018)[305]
United Nations Institute for Disarmament Research ('UNIDIR')	Multi-stakeholder	UNIDIR is an autonomous institute within the UN designed to generate ideas and action on disarmament and security. It comprises representatives of States, international organizations, civil society, the private sector and academia.[306]	UNIDIR acted as the expert consultant to the 2009-2010,[307] 2012-2013,[308] 2014-2015,[309] and 2016-2017[310] UNGGEs. UNIDIR acts as the expert consultant to the United Nations Group of Governmental Experts on Further Practical Measures for the Prevention of an	• Perspectives on Cyber War: Legal Frameworks and Transparency and Confidence-Building (Research Project 2011-2012)[312] • National Capabilities, Doctrine, Organization and Building Transparency and Confidence for Cyber Security: An Assessment (Research Project 2012-2013)[313] • Cyber Index Tool (Research Project 2012-2015)[314] • International Law and State Behaviour in Cyberspace Meeting

[301] https://documents-dds-ny.un.org/doc/UNDOC/GEN/G16/095/12/PDF/G1609512.pdf?OpenElement

[302] https://documents-dds-ny.un.org/doc/UNDOC/GEN/G16/156/90/PDF/G1615690.pdf?OpenElement

[303] https://undocs.org/A/HRC/35/22

[304] https://undocs.org/en/A/HRC/34/60

[305] https://documents-dds-ny.un.org/doc/UNDOC/GEN/G18/096/72/PDF/G1809672.pdf?OpenElement

[306] http://www.unidir.org/

[307] http://www.unidir.org/programmes/security-and-technology/support-for-the-group-of-group-of-governmental-experts-on-developments-in-the-field-of-information-and-telecommunications-in-the-context-of-international-security-2009-2010

[308] http://www.unidir.org/programmes/security-and-technology/support-for-the-group-of-governmental-experts-on-developments-in-the-field-of-information-and-telecommunications-in-the-context-of-international-security-2012-2013

[309] http://www.unidir.org/programmes/security-and-technology/support-for-the-group-of-governmental-experts-on-developments-in-the-field-of-information-and-telecommunications-in-the-context-of-international-security-2014-2015

[310] http://www.unidir.org/programmes/security-and-technology/support-for-the-group-of-governmental-experts-on-developments-in-the-field-of-information-and-telecommunications-in-the-context-of-international-security-2016-2017

[312] http://www.unidir.org/programmes/security-and-technology/perspectives-on-cyber-war-legal-frameworks-and-transparency-and-confidence-building

[313] http://www.unidir.org/programmes/security-and-technology/national-capabilities-doctrine-organization-and-building-transparency-and-confidence-for-cyber-security-an-assessment

[314] http://www.unidir.org/programmes/security-and-technology/the-cyber-index-tool

Entity/Initiative	Structure	Background	Connections to Other Stakeholders on Cyber	Key Outputs Relevant to Cyber-Governance
			Arms Race in Outer Space.[311]	Series (Research Project 2014-2015)[315] • Annual Cyber Stability Conference[316] • The Weaponization of Increasingly Autonomous Technologies (Research Project 2013-2015)[317]
United Nations Office on Drugs and Crime ('UNODC')	Intergovernmental	The UNODC is responsible for the Global Programme on Cybercrime, which is mandated to assist Member States to respond to cybercrime by providing capacity building and technical assistance.[318] The UNODC also convenes an open-ended United Nations Intergovernmental Expert Group on Cybercrime. The Expert Group was established by the UN Commission on Crime Prevention and Criminal Justice (which forms part of the UNODC) at the request of the UN General Assembly.[319] The Group held its first session in 2011, and has held subsequent sessions in 2013, 2017 and 2018.		• Report on the meeting of the open-ended intergovernmental expert group to conduct a comprehensive study of the problem of cybercrime held in Vienna from 17 to 21 January 2011 (2011)[320] • Report on the meeting of the Expert Group to Conduct a Comprehensive Study on Cybercrime held in Vienna from 25 to 28 February 2013 (2013)[321] • Comprehensive Study on Cybercrime (2013)[322] • Report on the meeting of the Open-ended intergovernmental Expert Group to Conduct a Comprehensive Study on Cybercrime, held in Vienna from 10 to 13 April 2017 (2017)**[323]** • Report on the meeting of the Open-ended intergovernmental Expert Group to Conduct a Comprehensive Study on Cybercrime, held in Vienna from 3 to 5 April 2018 (2018)**[324]** • Cybercrime Repository[325]
United Nations Economic Commission for Europe ('UNECE'),	Multi-stakeholder	The UNECE is one the UN's five regional commissions reporting to ECOSOC. The UNECE	The Task Force comprises representatives from other organizations	• Draft Recommendations on Cyber Security of the Task Force on Cyber

[311] http://www.unidir.org/programmes/security-and-technology/support-to-the-united-nations-group-of-governmental-experts-on-further-practical-measures-for-the-prevention-of-an-arms-race-in-outer-space

[315] http://www.unidir.org/programmes/security-and-technology/international-law-and-state-behaviour-in-cyberspace-meeting-series

[316] http://www.unidir.org/programmes/security-and-technology/annual-cyber-stability-conference

[317] http://www.unidir.org/programmes/security-and-technology/the-weaponization-of-increasingly-autonomous-technologies-phase-iii

[318] http://www.unodc.org/unodc/en/cybercrime/global-programme-cybercrime.html

[319] https://www.unodc.org/unodc/en/organized-crime/open-ended-intergovernmental-expert-group-meeting-on-cybercrime.html

[320] https://www.unodc.org/documents/treaties/organized_crime/EGM_cybercrime_2011/UNODC_CCPCJ_EG4_2011_3/UNODC_CCPCJ_EG4_2011_3_E.pdf

[321] https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/UNODC_CCPCJ_EG4_2013_3_E.pdf

[322] https://www.unodc.org/documents/organized-crime/cybercrime/CYBERCRIME_STUDY_210213.pdf

[323] https://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime-April-2017/Cybercrime_report_2017/Report_Cyber_E.pdf

[324] http://www.unodc.org/unodc/en/organized-crime/open-ended-intergovernmental-expert-group-to-conduct-a-comprehensive-study-of-the-problem-of-cybercrime2018.html

[325] https://sherloc.unodc.org/cld/v3/cybrepo/

Entity/Initiative	Structure	Background	Connections to Other Stakeholders on Cyber	Key Outputs Relevant to Cyber-Governance
Task Force on Cyber Security and Over-the-Air Issues		established the Task Force as an informal working group. It consists of representatives from States as well as other specialised organizations such as the ITU and non-governmental organizations.	(including the ITU) and non-governmental organisations..	Security and Over-the-air issues of UNECE (2018)[326]
World Bank Group	Group of international organizations	The World Bank Group is constituted by five organizations: the International Bank for Reconstruction and Development, the International Development Association, the International Finance Corporation, the Multilateral Investment Guarantee Agency, and the International Centre for Settlement of Investment Disputes. The World Bank was founded in 1944 and has 189 member States, which control the activities of the Bank through Boards of Governors and Executive Directors.[327]	To be a member of the World Bank, a State must be a member of the International Monetary Fund.	• Financial Sector's Cybersecurity: A Regulatory Digest (periodically updated)[328] • Financial Sector's Cybersecurity: Regulations and Supervision[329]
World Economic Forum	Multi-stakeholder	The World Economic Forum is an international organisation that was established in 1971.[330] In 2018, the World Economic Forum launched a Global Centre for Cybersecurity.[331]		• Partnering for Cyber Resilience (2012)[332] • Risk and Responsibility in a Hyperconnected World (2014)[333] • Partnering for Cyber Resilience Towards the Quantification of Cyber Threats (2015)[334] • Understanding Systemic Cyber Risk (2016)[335] • Advancing Cyber Resilience: Principles and Tools for Boards (2017)[336] • Cyber Resilience: Playbook for Public- Private Collaboration (2018)[337]

[326] https://www.unece.org/fileadmin/DAM/trans/doc/2018/wp29grva/GRVA-01-17.pdf
[327] http://www.worldbank.org/en/about/leadership/members
[328] http://pubdocs.worldbank.org/en/524901513362019919/FinSAC-CybersecDigestOct-2017-Dec2017.pdf
[329] http://documents.worldbank.org/curated/en/686891519282121021/pdf/123655-REVISED-PUBLIC-Financial-Sectors-Cybersecurity-Final-LowRes.pdf
[330] https://www.weforum.org/about/world-economic-forum
[331] https://www.weforum.org/press/2018/01/to-prevent-a-digital-dark-age-world-economic-forum-launches-global-centre-for-cybersecurity/
[332] http://www3.weforum.org/docs/WEF_IT_PartneringCyberResilience_Guidelines_2012.pdf
[333] http://www3.weforum.org/docs/WEF_RiskResponsibility_HyperconnectedWorld_Report_2014.pdf
[334] http://www3.weforum.org/docs/WEFUSA_QuantificationofCyberThreats_Report2015.pdf
[335] https://www.weforum.org/whitepapers/understanding-systemic-cyber-risk
[336] http://www3.weforum.org/docs/IP/2017/Adv_Cyber_Resilience_Principles-Tools.pdf
[337] https://www.weforum.org/reports/cyber-resilience-playbook-for-public-private-collaboration

Entity/Initiative	**Structure**	**Background**	**Connections to Other Stakeholders on Cyber**	**Key Outputs Relevant to Cyber-Governance**
				• Our Shared Digital Future Building an Inclusive, Trustworthy and Sustainable Digital Society (2018)[338] • Industrial Internet of Things: Safety and Security Protocol (2018)[339] • Innovation-Driven Cyber-Risk to Customer Data in Financial Services (2018)[340]

[338] https://www.weforum.org/reports/our-shared-digital-future-building-an-inclusive-trustworthy-and-sustainable-digital-society

[339] https://www.weforum.org/whitepapers/industrial-internet-of-things-safety-and-security-protocol

[340] https://www.weforum.org/whitepapers/innovation-driven-cyber-risk-to-customer-data-in-financial-services