The UN Global Digital Compact (GDC), achieving a trusted, free, open, and secure internet: trust-building

Wylde, Allison

Published in:
Proceedings of the 22nd European Conference on Cyber Warfare and Security, ECCWS 2023

DOI:
10.34190/eccws.22.1.1448

Publication date:
2023

Document Version
Publisher's PDF, also known as Version of record

The UN Global Digital Compact (GDC), Achieving a trusted, free, open, and Secure Internet: Trust-building

Allison Wylde
Glasgow Caledonian University (London)

allison.wylde@gcu.ac.uk

Abstract: A United Nations' (UN) public consultation, underway, is reviewing requirements for the Global Digital Compact (GDC) to advance UN goals for an 'open, free, and secure digital future for all' (UN, GDC, 2022). Achieving the goals relies on proposed principles, including: connecting everyone; avoiding fragmentation; protecting data; applying human rights; accountability for discrimination and misleading content; regulation of artificial intelligence; digital commons as a public good; and 'other' areas. The purpose of this paper is to present an argument that trust must be included as a central 'other' principle. Although successful achievement of the GDC goals is contingent on building trust in each principle, a method for trust-building is not provided. Through leveraging well-established organization and conflict management trust-building literature the contribution of this paper presents a fresh conceptual framework, allowing trust and trust-building in the goals to be operationalized and assessed. In, addressing the research gap as to how build trust in the GDC goals as they are implemented, the novel trust-building process as presented helps policymakers, practitioners, and academics better address potential risks to the future internet, such as, increased; state isolation, sovereignty, and internet fragmentation. Limitations and calls for further research highlight that understanding state-level trust-building in policy is not yet mature. Further, scholars needs to better categorize the processes, dynamics and norms involved in state-level trust-building, helping to counter future internet challenges.

Keywords: United Nations (UN), Global Digital Compact (GDC), internet, trust, institutional trust, cyber security, digital futures, future internet

1. Introduction

The UN has highlighted "stark and urgent problems facing all of humanity" and the "breakdown of trust and solidarity in one another" (UN, CA, 2021, p.4). In response they propose a Global Digital Compact (GDC) to achieve an open, free, and secure internet (UN, GDC, 2022). Eight principles are proposed: connecting everyone; protecting data; applying human rights; digital commons as a public good; regulation of artificial intelligence; accountability for discrimination and misleading content; avoiding fragmentation; and 'other' areas (UN, GDC, 2022); which provide a list of dos and don'ts, and a theoretical basis (public goods) to achieve goals. This paper argues that as the GDC goals are founded on trust, and the UN calls for trust-building (UN RDC, 2020: UN, CA, 2021), trust should be incorporated as a central integrating principle.

This paper argues that by positioning trust as a central and integrating principle; the goals can be delineated and evaluated. The contributions of this paper, propose an argument that trust be included as the 'other' principle, and address the question of building trust; well-established organizational and conflict resolution trust-building theory are leveraged to allow evaluation of the implementation of the GCU goals.

This section, the introduction, is followed by section 2, which explores, key challenges in East-West states' interpretations of norms, sovereignty and internet fragmentation, as examples of internet weaponization; followed by a discussion on the UN's calls for trust, followed by possible scenarios for the future internet. Section 3, reviews trust-building theory; with a focus on how trust can be understood, leveraged, and operationalized to assess goals are implemented. Section 4 presents an analysis of trust. Finally, in section 5, the conclusion, contribution, limitations, and promising directions for future studies together with the paper's implications are presented.

2. Achieving an open, free, and secure internet: the challenges and the goals

Key challenges face the internet, arguably acting as drivers behind the establishment of the GDC goals. What follows is not a systematic state of the art, rather an attempt to reach a concise understanding with the focus on relevant material.

2.1 Challenges to our digital futures

Since the 1980's when the web emerged the ethos has shifted from open-source and benevolence to increased deliberate, malicious actions, including state-sponsored hacking, criminal behaviour, harassment and attacks on the internet's structure (The Guardian, 2019): resulting in weaponizing the internet (Henriksen, 2019).

Prominent examples include the actions of advanced persistent threat actors (APTs); WannaCry and Not Petya, and breaches such as SolarWinds.

2.1.1 Actions of state-actors

Challenging relations among major state-actors including China, Russia and the US/EU/UK have emerged, arguably related to state doctrine. From 2013, in high-level government experts' meetings (GGE), the UN has called for international laws, human rights and fundamental freedoms (freedom of expression) to apply in ICT (GGE, 2013: GGE, 2015); alongside promoting cyber norms for predictability (hence trust) in the internet and ICT (Henriksen, 2019). UN's proposed cybercrime convention, in development for 2024, is challenged by some states. Russia opposes including human rights in the convention, suggesting that while human rights are enshrined in fundamental documents of the UN, individual states' must have rights take measures in accordance with their domestic laws (UNDOC, 2023a). This approach appears consistent with China and Russian previous actions in rewriting existing normative frameworks (Henriksen, 2019); considered next.

Russia as a GGE member promotes ideas such as the primacy of states in maintaining secure and peaceful ICT environments, territorial integrity (UNDOC, 2023a), and national information space (Claessen, 2020). Russia also contests UN norms and is attempting to centralize control and sovereignty through state legislation (Russian State Duma, 2018, in Claessen, 2020). By amending existing laws (Epifanova, 2020), Russia seeks to limit, register, and secure internet traffic through the creation of a duplicate infrastructure (Claessen, 2019). Amendments include compulsory installation of threat countermeasures, border control for connection lines crossing the Russian border and a Russian register of domain names (Epifanova, 2020). Russian also uses surveillance and isolation of its internet, as precedents for other states (Epifanova, 2020: Claessen (2019). Use of the term information rather than cyber by Russia, enables information security to encompass information-psychological and information-technical: arguably, a cyber arms race, to seek arms-control agreements (Henriksen, 2019). Current challenges by these state-actors and their allies, to the UN's proposed 2024 cybersecurity convention (UN, 2023) could result in a dilution of the provision for human rights, confusion over definitions and weakened capacity for responses to criminal actions (GDP, 2023). At the same time, China has sought to normalize human rights violations through rewriting human rights normative frameworks from obligations (Henriksen, 2019) to ideas that human rights are negotiable (Currie, 2023).

For the EU, the distributed denial of services (DDoS) attacks on Estonia shifted the EU's view from global multi-stakeholder cooperation for internet oversight to a position of global cyber security (EU, 2011, in Claessen, 2019; Schmidt, 2013). The EU propose a common approach to critical infrastructure security and engagement through public-private partnerships (Claessen, 2019).

Arguably the different approaches by states have culminated in UN calls for goals of an open, free, and secure digital future for all (UN, GDC, 2022). Key content in the calls includes trust and trust-building , trust in digital identities and integrity in finance and tax, set out in Table 1, below, and discussed next.

2.2 UN responses: calls for trust

Responding to challenges facing the internet, the UN has proposed policy actions, measures, and principles, all of which cite trust. Given limitations in scope, this discussion clarifies the calls for trust from the UN Secretary-General's Roadmap for Digital Cooperation (UN, RDC, 2020); Our Common Agenda (UN, CA, 2021); and, finally, the Technical Envoy's Office, Global Digital Compact (UN, GDC, 2022). Although UN Sustainable Development Goals (SDGs) framework, notably, SDG 16, Peace, Justice, and Strong Institutions and, SDG 17, Partnerships for the Goals (UN, SDG, n.d.) and the forthcoming 2024 UN cybersecurity convention (UNOCD, 2023b) are acknowledged; this paper confined to examining UN calls for trust and trust-building (UN, RDC, 2020: CA,2021: UN, GDC, 2022).

Drawing on earlier commitments the 2015 GGE aims to maintain peace stability, promoting an open, secure, peaceful, and accessible ICT environment based on non-binding state behaviour, founded on norms (Assembly, UG, 2015; GA, 2013, cited in Broeders et al., 2021). The framework is includes (1) no-interference with the public core of the internet (2) protecting electoral services (3) avoiding tampering (4) non commandeering of ICT devices (botnets) and (5) reduction and mitigation of significant vulnerabilities (UN, SG Panel, 2019). As an observation, these norms are largely limiting norms (UN, GDC, 2022).

Policy on preventative measures was replaced by ideas of good practices and positive duties (UN, GDC, 2022). In 2020, during the UN's 75th anniversary, a Roadmap for Digital Cooperation was released; based on, connect,

respect, and protect, with actors adhering to goals of: an inclusive digital economy and society; global connectivity; digital public goods; and, digital inclusion (UN, RDC, 2020). These actions promote open-source software, open data, open AI models, open standards, open content and the adherence to laws, standards, and best practices (UN, RDC, 2020). Specialist groups established to support the goals, includes, the digital public goods alliance (digitalpublicgoods.net, 2022) to promote positive actions including monitoring connectivity, digital inclusion, capacity building, trust-building, and oversight of AI (UN, RDC, 2020).

Subsequently in 2021, the Common Agenda aimed to protect the online space and strengthen governance (UN, CA, 2021). The Common Agenda's Commitments include: (1) leave no one behind; (2) protect our planet; (3) promote peace and prevent conflict; (4) abide by international law and ensure justice; (5) place women and girls at the centre; (6) build trust; (7) improve digital cooperation; (8) upgrade the UN; (9) ensure sustainable financing; (10) boost partnerships; (11) listen to and work with youth; and, (12) be prepared (UN, CA,2021).

Specifically, in the CA, commitments aim to improving digital cooperation, ensure that governance keeps pace and protecting online space, and through formation of the Internet Governance Forum, to innovate, reform and support effective governance of the digital commons (UN, CA, 2021). The key trust related actions, goals and principles in the policies are summarized below to allow comparison across the three policies (Table 1, below).

In summarizing the comparison of trust statements in the three policies (UN, RDC, 2020: CA,2021: UN, GDC, 2022); the trust elements are largely in parallel. In contrast with the earlier limiting behaviours, calls for non-binding norms seek to build on good practices and focus on positive duties (Table, 1, above). Examples of trust aims include building global cooperation, commitment (notably, UN RDC, 2020) and working in partnership (CA,2021). However, the policy documents are silent on the practical steps to achieve these aims.

Although minor differences are acknowledged, though, building trust (UN RDC, 2020: CA,2021: UN GDC, 2022) and enhancing trust (UN, RDC, 2020) as compared with tackling and addressing trust (CA,2021: UN, GDC), the scope of three documents are consistent in terms of trust, integrity, digital identity technology and silence on guidance on the processes involved in operationalizing trust and trust-building (UN RDC, 2020: CA,2021: UN GDC, 2022).

2.3 Possible futures for the internet

As discussed earlier in section 2.2, continued current tensions between competing state doctrines result in challenges to the internet, including: fragmentation of the internet, human rights abuses, state surveillance and election interference. What may happen next in terms of the future of the internet can be viewed through three scenarios and resulting actions: increased polarization towards state sovereignty; increased internet fragmentation; potentially countered by, entrepreneurs promoting and facilitating trust-building in cyber norms such as the GDC. Given space constraints the next section is confined to the possible impacts of each scenario.

Should current trends towards state sovereignty persist, state-actors harden their laws and norms of political and military responses, risking spillover into 'above-threshold' actions that could prompt military responses.

Table 1. Comparison of the key trust statements (summarized) in the Roadmap for Digital Cooperation (DC, 2020), the Common Agenda (CA,2021) and the Global Digital Compact (UN, GDC, 2022).

UN, RDC (2020)	UN, CA (2021)	UN, GDC (2022)
n=15 [21]	n=43 [47]	n=4
Promote engagement with and prioritise digital trust	Build and rebuild trust	Build trust and address, digital trust, and insecurity
Build global commitment to and enhance trust, trust in technology, in digital identity and in trustworthy AI	*Build integrity, *Improve experience with public infrastructure and basic services, *Inclusive listening, *Tackle corruption, *Reform tax, *Financial integrity	Inequality leads to mistrust between countries and mistrust in institutions
Prioritize trust and security	work in partnership to build trust	address digital trust and security
Note, n = equals the number of times trust (in context) appears in each document; where a [number] is shown, this is the total observations, including material that has been excluded as not relevant to the context.		

Continued internet fragmentation can be viewed as impacting across two levels. At the level of inter-state relations, fragmentation could result in state isolation. At the level of citizen, state actions could interfere in election, or through surveillance of citizens, could drive down rights and freedoms. These impacts longer term could lead to further deteriorating relations.

Conversely, should the influence of norm entrepreneurs' increase, impacts of the former two scenarios could be reduced. As norms evolve increased levels of cooperation and trust results, in part due to familiarity and increased utility (Wylde, 2022). The benefits could reduce friction between states generating increasing returns on engaging in cooperation.

2.4 Summary

From the perspective of the UN GDC, the dominance of policy, goals and principles rests on positive actions, the "dos" as compared with the single "don't" principle, avoiding internet fragmentation. Secondly, and in contrast, current and future challenges highlight emerging state calls for sovereignty and moves towards internet fragmentation. Arguably and thirdly, this demonstrates the need for norm entrepreneurs to cooperate and strengthen a message of the economic utility of trust between states. Whether this future approach based on cooperation will develop trust (or not) remains unclear. The next sections reviews trust-building in the GDC goals (UN, GDC, 2022).

3. Achieving the GDC goals: trust-building theory

As highlighted in Table 1 above, although the selected policy documents all refer to trust, building trust and trustworthiness (as well as related terms), are not explicit. In the discussion that follows, prominent trust and trust-building theory is discussed, followed by the first steps towards a conceptual framework to allow an assessment of trust in policy to be undertaken.

3.1 Trust and trust-building theory

Although trust is well researched and conceptualized among organization and management scholars (notably Mayer et al., 195; Rousseau et al., 1998) and from conflict resolution (Deutsch, 1958), this paper argues that in policymaking, little guidance is provided on definitions of trust and the operationalization of trust-building. In addressing this research gap, understanding leveraging, and operationalizing trust theory is presented. Given space limitations, a state of the art is not presented, rather a focused discussion on key theory provides a framework for evaluation.

Trust is a construct that operates in and at different levels across different entities, for example, at the level of individual trustor-trustee relations, or trust in teams, or trust at an organizational or institutional level (Fulmer and Gelfand, 2012). Trust also exits beyond trustor' relations, as trust in technology (McKnight, 2011) and trust in institutions (Bachman and Inkpen, 2011: Rousseau et al., 1998). The paper aims to understand trust in institutional policies, principles, and trust in 'applying human rights' (UN, GDC, 2022). Institutional trust is based on favourable assumptions by a trustor of a trustees' future behaviour. Trustors' trust institutions, their norms, and patterns of behaviour (Bachmann and Inkpen, 2011). Institution-level trust, provides organizational supports (such as legal systems), reduces vulnerability for trustors (Rousseau et al., 1998) and relies on trusted people in organizations (Vanneste, 2016)

This paper defines trust as based on positive expectations by a trustor that a trustee will perform an action, irrespective of trustor' control or monitoring, trust requires a trustor to accept vulnerability (Mayer et al., 1995: Rousseau et al., 1998); moderated by a trustor's propensity to trust (Mayer et al., 1995), ability to trust and trust experience (Deutsch, 1958). This definition allows for evaluation of antecedents, processes, and outcomes of trust (Wylde, 2021); the conceptual framework is presented next.

3.2 Trust analysis: conceptual framework

Trust, in an institutional concept, such as a goal or a principle, is next evaluated, through drawing on two major approaches from trust-building theory, organization and conflict studies. The aim is to evaluate trust in UN goals, principles, positive actions and best practices along with one limiting principle (avoiding internet fragmentation) and theory (UN, GDC, 2022).

The frame of analysis draws from the well-established integrative trust model first proposed by Mayer at al. (1995), in organization and management studies together with Deutsch's (1958) foundational work on trust in conflict resolution studies. The strengths of these approaches lie in their ability to provide a process-based view to assessing the construct of trust-building, in sometimes, contested relations, essential given the complexities of managing complex public problems (Oomsells and Bouckaer 2014). Utility of this approach is shown in recent Google Scholar searchers, terms the "Integrative trust model" returned about 2.75m results, and "Conflict resolution AND trust" returned about 2.6m (GoogleScholar.com, 08 Jan. 2023). The analysis framework separates, trust-antecedents, trust-assessments, and the post-trust actions (Table 2, below). Firstly, trust antecedents include positive expectations of a trustee's trustworthiness, moderated by propensity to trust (Mayer at al., 1995), plus the ability to trust, moderated by prior trust experiences (Deutsch, 1958). The trust assessment, second, evaluates the trustee's ability, benevolence, and integrity (ABI) (Mayer et al., 1995). ABI is explained as ability (capability to undertake a specific task), benevolence (goodwill), and finally, integrity (honesty). Thirdly, following trust, a trustor's accepts vulnerability and takes a risk, as set out in table 2 below.

The strengths of this conceptual process framework lie in its ability to disentangle complex, dynamic and interlinked elements into a process allowing trust to be assessed. Further, by conceptualizing trust as occurring at an institutional level, vulnerability and risk are reduced (Mayer et al., 1995); through trusting policy (Bachman and Inkpen, 2011: Rousseau et al., 1998) and the organizations' people (Vanneste,2016).

Table 2. Trust-building process model, viewed from the perspective of a trustor (source the author, developed from Mayer et al., 1995: Deutsch, 1958: Wylde 2021)

Antecedents to trust	Trust assessment	Post-trust actions
Ability to trust	Ability	Acceptance of vulnerability
Trust, prior experience	Benevolence	
	Integrity (ABI)	
	Assessment of risk	Risk-taking behavior
Mediated by propensity	Mediated by propensity	Mediated by propensity

4. The goals and principles: assessing trust

In achieving a free, open and secure digital future eight principles are proposed for stakeholders (UN, Tech Envoy, 2022); the conceptual framework proposed in table 2 is applied.

Given the complexities in managing societal issues (Oomsells and Bouckaer 2014) this paper adopts a process-based approach to disentangle the separate elements of trust (Wylde, 2021) to help understand what is involved in securing the UN goals. What follows next is a simplified set-by-step process to the assessment of trust in the key trust elements as summarized in Table 1. This is followed by a trust assessment of the state of trust in three key state-actors involved in UN GGE talks, China, Russia, and the US.

4.1 Trust assessment

As a start, the antecedents of trust are provided by UN calls for an open and secure internet (UN, RDC, 2020 CA, 2021), reliant on trust, building trust and trustworthy frameworks (Table 1). These examples provide evidence for the presence of presumptive trust and an ability to trust in the goals. At the same time, stakeholders cooperate through partnerships to achieve these goals; demonstrating a propensity to trust.

In the next stage assessment of trust, the propensity to trust is assumed to reflect presumptive trust on the part of the trustor (Table 2). A trustor assesses the policy or principle based on its ability (can the policy achieve its task?) benevolence (do the policy intentions demonstrate goodwill towards stakeholders?) and integrity (does the policy demonstrate honesty) cf., Mayer et al. (1995). From conflict resolution considerations include prior experiences of trust and ability to trust (Deutsch, 1958); supported by institutional trust (Bachmann and Inkpen, 2011: Rousseau et al., 1998: Vanneste, 2016)

If the ABI elements are assessed favourably, the final step is trust formation, with a caveat, as trust requires a trustor's acceptance of vulnerability (Table 2). In institutional trust, trustors are predisposed to trust institutions (and their people), thereby reducing vulnerability (Bachmann and Inkpen, 2011: Rousseau et al., 1998: Vanneste, 2016); resulting in an increased likelihood of trust in the policy or principle.

4.2 Operationalizing the assessment of the trust-building

An assessment state of trust among three key players, China, Russia, and the US is presented next. In examining the antecedents of trust, state-actors Russia and America can be considered as sharing a common Cold War history and experience while China, experienced a cultural revolution. These experiences may act as an antecedent, predisposing these states to a propensity that is closer to distrust, trust and verify (Lewicki, 1998) and zero trust (Wylde, 2021).

In terms of the ability to trust, although the US, UK and other western democracies hold free elections, Russia, Iran, and North Korea are accused with election and referendum interference (O'Connor et al., 2020) resulting in a loss of trust in the election process (O'Connor et al., 2020). Actors experiencing election interference may have their ability to trust negatively impacted.

Fukuyama considers that culture is also important, for example, individuals in China, may be more likely to be predisposed to trusting family above state-actors, arguably due to experiences of distrust in state-actors and institutions (Fukuyama, 1996).

As institutional trust is in question; actors may be considered to possess favourable predispositions, though impacted negatively through prior experiences.

4.3 Summary

By simplifying the steps involved in assessing trust in a goal or a principle through drawing on the process model (Table 2). An assessment of trust among the major state-actors can be undertaken. Pointing to the value in leveraging well-established trust theory to disentangle the complex processes and dynamics involved in trust. Once trust is assessed, any deficit in trust can be identified and recommendations for trust-building can follow, based on the steps outlined. To the best of the author's knowledge, this is the first attempt at assessing trust in policies (goals and principles) as operationalized, evaluated and monitored.

5. Conclusion

The contribution and limitations of the paper, followed by promising directions for future studies, and the implications, are presented next.

In addressing questions of trust in policy, this paper examined and reviewed important challenges faced by the internet together with implementation of UN goals/ principles, and possible future internet scenarios. The paper presents an argument that to achieve the GDC goals, trust must be included as a central principle.

In examining key challenges to the internet: emerging state calls for sovereignty and moves towards internet fragmentation were identified. The paper highlighted the importance of cooperation between norm entrepreneurs in norm implementation along with communication of the economic utility of state-to-state trust.

The research gap was addressed through the contribution which leveraged well-established trust and conflict management theory to create a conceptual framework. This allowed the complex processes and dynamics involved in trust-building to be disentangled. Next, the framework was operationalized to evaluate trust in policy among the major state-actors. Findings suggest that actors may starting from a position of distrust (or zero trust). The paper argues trust assessment allows gaps in trust to be identified and recommendations for trust-building provided, therefore further demonstrating the importance in understanding the steps involved in trust-building and categorizing the processes involved.

These first steps towards a trust-building conceptual framework (Table 2) aim to provide a consistent approach to assessing and categorizing trust. Recognising the multifaceted processes and elements involved in trust and trust-building the contribution helps as policy is operationalized, and trust is evaluated and monitored.

As with all research limitations are inevitable, for example, given time/ space limitations, the evaluation focused on three linked UN policies. Nevertheless, the work presented here suggested that UN policy is inter-linked. Through consideration of potential scenarios for the future internet, important directions for future research suggest the importance of examining potential future state responses and actions. This would allow better understanding of the phenomena of trust-building among state-actors. Interesting avenues to pursue research concern identifying the specific actions that build trust among state-actors. Follow-on studies could consider the implementation of trust-building actions, for example, to reduce polarisation, sovereignty and/ or internet

fragmentation. Finally, examining trust-building measures as they play out in supporting the actions of entrepreneurs and norms on policy formation.

Should these findings prompt other researcher's interest future work could explore the nature of the trust amongst the policymakers involved in setting the agenda, and the role of citizens, in terms of trusting policy and/ or policy adoption. This would help policymakers understand the likely make-up and take-up of policy and to assess whether pilot testing or amendments may be necessary.

Acknowledgements

Thank you to university and industry colleagues for helpful discussions, challenging thoughts and help with the final version of the paper.

References

Accessnow. (n.d.) "Supreme court of India rules to restrict access to the worlds largest digital identity framework Aadhaar", [online]. https://www.accessnow.org/supreme-court-of-india-rules-to-restrict-worlds-largest-digital-identity-framework-aadhaar-but-debate-continues/ [Accessed 08 Jan. 2023].

Assembly, U.G. (2015) "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. Seventieth Session, Item, 93", [online]. https://documents-dds-ny.un.org/doc/UNDOC/GEN/N15/228/35/PDF/N1522835.pdf [Accessed 08 Jan. 2023].

Bachmann, R. and Inkpen, A. C. (2011) "Understanding Institutional-based Trust-building Processes in Inter-organizational Relationships", Organization Studies 32, pp. 281–301.

Broeders, D. (2021) "The (im)possibilities of addressing election interference and the public core of the internet in the UN GGE and OEWG: a mid-process assessment", Journal of Cyber Policy, 6(3), pp. 277-297. DOI: 10.1080/23738871.2021.1916976

CA. 2021. "The United Nations, Our common Agenda", [online]. https://www.un.org/en/content/common-agenda-report/assets/pdf/Common_Agenda_Report_English.pdf [Accessed 08 Jan. 2023].

Claessen, E. (2020) "Reshaping the internet - the impact of the securitisation of internet infrastructure on approaches to internet governance: the case of Russia and the EU", Journal of Cyber Policy, 5(1), 140-157. DOI: 10.1080/23738871.2020.1728356

Currie, K.E. (2023) "Prevent China from killing human rights at the UN", Foreign Policy, 247, pp. 5–7, [online]. https://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=161154883&site=ehost-live&scope=site [Accessed 17 Feb. 2023].

Deutsch, M. (1958) "Trust and suspicion", The Journal of Conflict Resolution, 2(4), pp. 265-79.

digitalpublicgoods.net. 2022 "Promoting Digital Public Goods to promote a more inclusive world", [online]. https://digitalpublicgoods.net/ [Accessed 08 Jan. 2023].

Epifanova, E. (2020) "Deciphering Russia's sovereign internet law", German Council on Foreign Relations 16/Jan/2020, [online]. https://dgap.org/en/research/publications/deciphering-russias-sovereign-internet-law [Accessed 17 Feb. 2023].

EU (2012) "European Parliament resolution 12/Jun/2012 on critical information infrastructure

protection-achievements and next steps: towards global cyber-security" (2011/2284(INI)) https://www.europarl.europa.eu/doceo/document/TA-7-2012-0237_EN.pdf [Accessed 17 Feb. 2023].

Fulmer, A. and Gelfand, M. (2012) "At what level (and in whom) we trust: trust across multiple organizational levels", Journal of Management, 38(4), pp. 1167-1230.

Fukuyama, F. (1996) "Trust: The social virtues and the creation of prosperity", New York: Simon and Schuster.

Henriksen, A. (2019) "The end of the road for the UN GGE process: The future regulation of cyberspace", Journal of Cybersecurity, 5(1), 2019, tyy009, [online]. https://doi.org/10.1093/cybsec/tyy009 [Accessed 17 Feb. 2023].

hlpf.un.org. (2022) "Preserving an open Internet to achieve the SDGs: The Internet as an enabler for achieving SDGs 4 and 5", [online]. https://hlpf.un.org/2022/programme/preserving-an-open-internet-to-achieve-the-sdgs-the-internet-as-an-enabler-for [Accessed 08 Jan. 2023].

Lewicki, R.J., McAllister, D.J. and Bies, R.J. (1998). Trust and distrust: New relationships and realities. Academy of management Review, 23(3), pp.438-458.

Mayer R., Davis, J. and Schoorman, F. (1995) "An integrative model of organizational trust", Academy of Management Review, 20(3), pp. 709-734.

McKnight, D.H., Carter, M., Thatcher, J.B. and Clay, P. (2011) "Trust in a specific technology: an investigation of its components and measures", ACM Transactions on management information systems, 2(2), pp. 1-25.

Mir, U. B., Kar, A. K., Dwivedi, Y. G., Gupta, M. P. and Sharma, R. S. (2020) "Realizing digital identity in government: Prioritizing design and implementation objectives for Aadhaar in India", Government Information Quarterly, 37(2), [online]. 101442. doi.org/10.1016/j.giq.2019.101442 [Accessed 08 Jan. 2023].

O'Connor, S., Hanson, F., Currey, E. and Beattie, T. (2020) "Cyber-enabled foreign interference in elections and referendums", Canberra: Australian Strategic Policy Institute.

Oomsels, P. and Bouckaert, G., 2014. “Studying interorganizational trust in public administration: A conceptual and analytical framework for" administrational trust", Public Performance & Management Review, 37(4), pp. 577-604.

Rousseau, D.M., Sitkin, S.B., Curt, R.S. and Camerer, C. (1998) "Not so different at all: a cross discipline view of trust", Academy of Management Review, 23(3), pp. 393-404.

SDG.IISD.ORG (2021) SDG knowledge Hub, [online]. https://sdg.iisd.org [Accessed 08 Jan. 2023].

Russian State Duma. (2019) “On the Introduction of Changes into the Law on Information, Information Technologies and on the Protection of Information”, in Claessen, E. (2020) “Reshaping the internet - the impact of the securitisation of internet infrastructure on approaches to internet governance: the case of Russia and the EU”, Journal of Cyber Policy, 5(1), 140-157. DOI: 10.1080/23738871.2020.1728356

Schmidt, M. N. (2013) “Tallinn Manual on the International Law Applicable to Cyber Warfare”, New York: Cambridge University Press.

The Guardian. (2019) "Tim Berners Lee on 30 years of the web", [online]. https://www.theguardian.com/technology/2019/mar/12/tim-berners-lee-on-30-years-of-the-web-if-we-dream-a-little-we-can-get-the-web-we-want [Accessed 08 Jan. 2023].

The Register. (2022) "Indian authorities conflicting Aadhaar advice", [online]. https://www.theregister.com/2022/05/30/indian_authorities_conflicting_aadhaar_advice/ [Accessed 08 Jan. 2023].

UN, CA, 2021. “United Nations, Our Common Agenda”, [online]. https://www.un.org/en/common-agenda [Accessed 08 Jan. 2023].

UN, GDC. 2022. "The United Nations, Tech Envoy's Office, Global Digital Compact", [online]. https://www.un.org/techenvoy/global-digital-compact [Accessed 08 Jan. 2023].

UN, ODC. (2022a) “Cybercrime ad hoc committee, no.3, Statement by the Russian Federation”, 29/Aug.-09/Sept./2022, [online].

https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Third_session/Documents/Statements/Item6/Russian_Federation_6_E.pdf [Accessed 18 Feb. 2023].

UN, ODC. (2022b) “Cybercrime ad hoc committee, no.3, Main session”, 29/Aug.-09/Sept./2022, [online]. https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/ahc_third_session/main.html [Accessed 18 Feb. 2023].

UN, RDC. (2020) "The United Nations, GA Roadmap for digital cooperation: implementation of the recommendations of the high-level panel on digital cooperation", [online]. https://documents-dds-ny.un.org/doc/UNDOC/GEN/N20/102/51/PDF/N2010251.pdf?OpenElement [Accessed 08 Jan. 2023].

UN, SDG. (n.d.) "The United Nations, Sustainable Development goals", [online]. https://sdgs.un.org/goals [Accessed 08 Jan. 2023].

UN, SG Panel. (2019) "UN Secretary General's High-Level Panel on Digital Cooperation", [online]. https://www.un.org/en/sg-digital-cooperation-panel [Accessed 08 Jan. 2023].

UN, Tech Envoy. (2022) "Contribute to the Global Digital Compact: A How-to-Guide (version 17 October 2022)", [online]. https://www.un.org/techenvoy/sites/www.un.org.techenvoy/files/Global-Digital-Compact_how-to-engage-guide.pdf [Accessed 08 Jan. 2023].

Vanneste, B.S. (2016) "From interpersonal to interorganizational trust: the role of reciprocity", Journal of Trust Research, 6(1), pp. 7-36.

Wylde A. (2022) “Cyber Security Norms: Trust and Cooperation,” Conference paper. ECCWS 2022.

Wylde, A. (2022) “Questions of trust in norms of zero trust”. In Intelligent Computing, Proceedings of the 2022 Computing Conference, 3, pp. 837-846. Cham: Springer International Publishing.