GENEVA DIALOGUE ON RESPONSIBLE BEHAVIOUR IN CYBERSPACE

Phase 1 Report

Professor Paul Cornish
Visiting Professor, LSE IDEAS, London School of Economics

Dr Camino Kavanagh
Visiting Fellow, King's College London

31st May 2019

EXECUTIVE SUMMARY

This Report covers Phase 1 of the Geneva Dialogue project on Responsible Behaviour in Cyberspace. The Report is presented in four sections:

Section 1: Background
The 2015 UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security stressed that an '*open, secure, stable, accessible and peaceful ICT environment* is essential for all and requires effective cooperation among States to reduce risks to international peace and security' and recommended a number of measures, '*including norms of responsible behaviour*', to promote that goal. Both italicised sets of ideas are defined and discussed, with key questions noted for subsequent review. **[Pages 4-5]**

Section 2: The Roles and Responsibilities of States in Cyberspace
Section 2 explores different understandings of responsible state behaviour in cyberspace. Principles and expectation of responsible state behaviour are very well developed in international law. The Report considers how responsible state behaviour has been understood by successive UN Groups of Governmental Experts (UN GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security. The report discusses the eleven non-binding 'Norms, Rules and Principles for the Responsible Behaviour of States' listed in the report of UN GGE 2015. Section 2 discusses various 'complementary expectations' which should be borne in mind when considering the roles and responsibilities of states: the perceived to maintain mutual, inter-state deterrence; constraints and opportunities arising from cross-border collaboration; and the requirements of capacity-building and technical co-operation. Section 2 concludes with a summary of points made during the November 2018 Geneva Dialogue Workshop. **[Pages 6-12]**

Section 3: Sharing Responsibility in Cyberspace
Section 3 examines the sharing of responsibility between States (as discussed in Section 2) and other non-state stakeholders and actors. The Report describes the sharing of responsibility between these different constituencies as a form of 'complex co-operation', allowing for the *quantitative* analysis both of the number of type of actors involved, and of the volume of data and information being distributed, as well as *qualitative* analysis of different forms of co-operation. Section 3 reviews the extant roles and responsibilities of Private Sector and Industry Actors and Civil Society and Other Key Actors respectively, and summarises points made during the November 2018 Workshop. **[Pages 13-21]**

Section 4: Overarching Analysis and Next Steps
The final section of the Report offers an overarching analysis in which it is suggested that a framework or 'regime' of responsibility in cyberspace is emerging which should contribute to greater peace, security and stability. Some refer to this framework as a 'stability framework'. Nevertheless, irresponsible (and malign) behaviour on the part of States persists and remains potentially destabilizing, prompting the authors to ask what incentives exist for promoting more responsible behaviour, and what costs might be associated with irresponsible behaviour. With a view to closing the perceived 'responsibility gap' between normative aspirations and actual practice (particularly on the part of states), the Report outlines a series of questions that could be addressed by the Geneva Dialogue and concludes by recommending 'Next Steps' for the Geneva Dialogue. **[Pages 22-26]**

The final pages of the report (**Annex 1**) are in the form of a table setting out some of the private sector and civil society actors are engaging with the norms recommended in the 2015 GGE report. This table is at an early stage of development but could serve as the basis of further analysis of the distribution of responsibility in cyberspace. **[Pages 27-29]**

INTRODUCTION

The Geneva Dialogue on Responsible Behaviour in Cyberspace was established by the Swiss Federal Department of Foreign Affairs to analyse the roles and responsibilities of three interrelated and interdependent constituencies – states, the private sector and other actors including civil society and academia – in contributing to an open, secure, stable, accessible and peaceful cyberspace as it bears upon international peace and security.

States carry primary and unrivalled – yet not absolute – responsibility for international peace and security. Several other actors also have concern for international peace and security and have discrete roles and responsibilities. In this regard, the objective of the Geneva Dialogue is to better understand the interaction of these roles and responsibilities as they relate to ICT in the context of international peace and security. It is clear that states cannot meet their responsibilities without engaging with these other actors, and vice versa. In this respect a sense of balance is called for. This is particularly the case where a state's responsibilities, or duties, towards other states as well as towards its nationals are concerned. Furthermore, as societies become increasingly dependent on ICT, so citizens want – and increasingly need – the benefits of the digital economy. Citizens expect the state to respect these rights while also expecting states to ensure their safety and security. This also calls for greater involvement and engagement by the private sector, and the technology sector in particular. In other words, where cyberspace is concerned there is now a very powerful, political, transactional and distributed dimension to our understanding of responsible behaviour. What states do – or fail to do – in this area can have a direct, immediate and serious effect on the public and on society domestically and internationally.

An initial discussion of the analysis undertaken in these areas took place at a workshop held in Geneva in November 2018. The workshop informed an overarching analysis, presented in this report, of the ways in which responsibility is shared (deliberately or otherwise) between different constituencies, constituting a 'responsibility regime' so to speak, that contributes to the maintenance of international peace and security in cyberspace.

STRUCTURE

This Report is structured in four sections. Section 1 provides a background discussion of key terms: 'peaceful, secure and stable cyberspace' and 'responsible behaviour'. Section 2 explains the roles and responsibilities of states in cyberspace in the context of international peace and security. Section 3 examines the sharing of roles and responsibilities of other actors in contributing to these efforts. Finally, Section 4 provides a summary analysis with observations concerning a possible second phase of the initiative.

SECTION 1: BACKGROUND

The 2015 UN Group of Governmental Experts (GGE) stressed that an "open, secure, stable, accessible and peaceful ICT environment is essential for all and requires effective cooperation among States to reduce risks to international peace and security"[1] and recommended a number of measures, including norms of responsible behaviour, to promote that goal. The GGE also noted that "adherence by States to international law, particularly their Charter obligations, is an essential framework for their actions in their use of ICTs and to promote an open, secure, stable, accessible and peaceful ICT environment"[2] and the importance of common understandings on how international law applies in this regard.

An open, secure, stable, accessible and peaceful ICT environment (otherwise understood as a functionally reliable international ICT environment in which international law and other norms are respected) could be defined as one which satisfies the following criteria:

- Non-exclusivity: all legitimate participants, undertaking legitimate activities, should be able to enjoy the benefits of cyberspace.
- Behavioural consistency: there should be a degree of predictability regarding the actions of states and non-state actors in cyberspace.
- Trustworthiness: there should be a general sense that in this environment as in any other, contracts properly made will be respected and binding.
- Positive incentives: cyberspace should be an environment in which cooperation and the avoidance of conflict is encouraged and rewarded.
- Negative incentives (i.e. disincentives): cyberspace should be an environment in which engagement in illegal, illegitimate, malicious or destructive activity is discouraged and punished in a manner consistent with existing international law and obligations of States.

An open question is whether states and other actors such as the private sector and civil society demonstrate a broadly similar understanding of 'an open, secure, stable, accessible and peaceful cyberspace', and whether this goal is a common objective within and across geographic regions.

In a rather circular way 'responsible behaviour' could be defined as behaviour by a given actor in a given set of circumstances that can be said to conform to the laws, customs and norms generally expected of that actor in those circumstances. For the purposes of this report, however, 'responsibility' is also suggestive of both obligation/duty and expectation and involves norms of both a legal and a non-binding (or voluntary) character. The latter can carry a great deal of political and moral force. In addition, 'responsible behaviour' can be said in general to be behaviour which conforms to public standards of transparency, integrity and accountability. Responsibility is thus a term with both 'hard' and 'soft' meanings. This is common to all human interaction, in all formats and on all levels. But it resonates particularly strongly with states – what, for example, are states *obliged* to do with regard to peace, security and stability in cyberspace; and what are states *expected* to do? States are familiar with the difference between legally binding commitments and those which are non-binding. Both are authoritative but in different ways: the former is a legal obligation undertaken to other states or organisations, in the form of a treaty or similar; the latter is more by way of a political expectation of action of a certain type (political, moral) or a positive duty (or good practice). In the former, the 'legitimacy of law' creates collective expectations of behaviour with the intention of "pull[ing] the behaviour of its subjects toward conformity to its contents".[3] In this regard, the law of treaties "encapsulates this compliance pull in its fundamental norm of *pacta sunt*

[1] United Nations General Assembly, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, A/70/174, 22 July 2015, para. 2: https://undocs.org/A/70/174 (UN GGE 2015).
[2] UN GGE 2015 para 25.
[3] M. Finnemore and D.B. Hollis (2016), 'Constructing Cyber Norms'. *The American Journal of International Law*, Vol. 110, No. 3 (July 2016), pp. 425-479

servanda", whereby "[e]very treaty in force is binding upon the parties to it and must be performed by them in good faith." A political commitment or voluntary norm may initially be of a non-binding character, but norms are dynamic, their meaning may shift over time and some may even be instantiated into law, becoming binding later on.[4] As this report will argue, states cannot be expected to meet these obligations and expectations alone and must therefore engage other actors. This in turn raises questions concerning the roles and responsibilities of these other actors. Relevant to all three constituencies is another question; whether responsibility is something to be regulated and enforced, or preferred and encouraged.

[4] Ibid.

SECTION 2: THE ROLES AND RESPONSIBILITIES OF STATES IN CYBERSPACE

Anchored in the work of the UN Groups of Governmental Experts, this section of the report explores different understandings of responsible state behaviour in cyberspace.

Context

While there are some states for whom the prospect of malicious ICT activity and conflict in cyberspace is a problem to be prevented, others see it as a strategic and economic opportunity to be exploited in that they choose to maintain the capacity for malicious activity in cyberspace that is potentially destabilizing and poses a risk to international peace, security and stability. A third group of states seek to occupy both categories simultaneously; shaping or adopting principles or norms of responsibility with regard to preventing the malicious use of ICT while also developing and maintaining such capacities. At the very least therefore, we can expect to see some attempt at balancing sharply conflicting policy/strategic imperatives.

This problem was reflected in the report of the 2015 UN Group of Governmental Experts (GGE) which noted disturbing trends in the global ICT environment, including "a dramatic increase in incidents involving the malicious use of ICT by State and non-State actors", and the possibility that these could be directed against the critical infrastructures and associated information systems of a state. It further noted that such trends "pose a risk for all States", and to international peace and security. It placed emphasis on the reality that numerous states are developing ICT capabilities for military purposes, increasing the likelihood of ICT use in conflict and that states are "rightfully concerned" about how these and related developments could lead to "destabilizing perceptions", increase the likelihood of conflict and cause harm to their citizens, property and economy.[5]

The number of ICT-related incidents involving states is increasing both in number and sophistication. These include state-supported acts of economic and industrial espionage, important data breaches targeting key government agencies and services and multi-national companies, and the technologically sophisticated surveillance practices of states, including the general surveillance of citizens. Also of growing concern are incidents involving acts of sabotage or disruption conducted by state actors or their proxies targeting critical infrastructure or seriously affecting essential services and the use of ICT to influence the domestic affairs of other states, including for political and strategic effect. To date, most of these activities have taken place outside the context of armed conflict. Governments have, nonetheless, increasingly turned their attention to those incidents that, although still conjectural, may result in loss of human life or significant and lasting damage to industrial facilities and infrastructure providing essential services to the public. Alongside challenges of attribution, these kinds of behaviours raise the stakes for miscalculation which, in the current international environment, is potentially destabilizing and could endanger international peace and security.

Concern is also mounting over the growing reliance by states on *offensive* ICT capabilities. Estimates of the number of countries possessing the capacity to conduct offensive ICT operations, or the intention to do so, range from about 20 to over 50.[6] It is, perhaps, not surprising that relatively few states admit publicly to owning and deploying such capacities although this trend appears to be shifting, perhaps in the hope that public announcements of such capacities and the declared intent to use them will have a deterrent effect. The ICT tools which would be necessary for an effective offensive cyber capability are more or less dual-use commodities, available for both defensive and

[5] UN GGE 2015, p.6.

[6] See, for example, the work undertaken by Digital Watch, showing those states (23 in March 2019) for which there is *evidence* ('in the form of official and publicly available documents issued by state institutions') of the development of offensive ICT capabilities and those states (30 in March 2019) for which there are *indications* ('from credible media or technical community sources') of the intention to develop such capabilities: https://dig.watch/processes/ungge#Armament

offensive action and could, as such, be at the disposal of many states. Nevertheless, it is reasonable to assume that uncertainty surrounding the capacity for offensive action could be the driver of emerging 'insecurity dilemmas' and destabilisation. For this reason alone, the rationale for diplomatic activity in this area is compelling. Finally, it is not only states that have access to both offensive and defensive cyber capabilities. Sub-state and non-state actors can also play a very significant role in this field and therefore present their own level and style of challenges.

Expectations of Responsible State Behaviour in Cyberspace

The notion of state responsibility under international law entails a state's responsibility for violating its obligations under international law. In this regard, exercising sovereignty is a right, not an obligation and international law does not discuss the "positive obligations/responsibilities" of states towards actively seeking certain objectives. Nonetheless, expectations of a state's external and internal responsibilities are strong. In the context of international peace and security a traditional and simple understanding of responsible state behaviour – i.e. the responsibilities we would expect a state to observe – would include the following:

- Responsibility for the safety and well-being of a state's nationals and those who find themselves in its territory, as well as nationals of other states in the event of conflict (these latter duties are inherent in international human rights and international humanitarian law).
- Responsibility to protect sovereign territory and interests; and maintain and grow a secure and strong national economy;
- Responsibility to other states and the international community as a whole.

These three sets of responsibilities, obligations and duties involve norms of both a legal and a non-binding (or voluntary) character. They can carry a great deal of political and moral force. As statements of general principle, all three sets of responsibilities should apply in all environments in which states are active, including cyberspace. In the latter vein, the UN Groups of Governmental Experts (GGEs) have made substantial progress in identifying a framework for the behaviour of states with respect to the use of ICT in the context of international peace and security. This framework is anchored both in existing international law as well as non-binding norms of behaviour. In short, it is understood that states need to ensure that their actions in cyberspace are carried out in conformity with their existing obligations under international law, including obligations under the UN Charter, international human rights and humanitarian law

The principle of responsibility as it applies to states has strong links to the concept of sovereignty, a simple definition of which might be 'unrestricted governmental authority within territorial boundaries.'[7] If sovereignty can be understood as a *right* to be enjoyed by states in the international system, then it clearly imposes a counterpart *obligation* on other states to guarantee that right and not to interfere in another state's sovereign authority. This exchange of rights and obligations is made explicit in the Charter of the United Nations in which Article 2.1 speaks of 'the sovereign equality of all members' and Article 2.4 insists that all members of the United Nations shall refrain 'from the threat or use of force against the territorial integrity or political independence of any state'. The 1970 Declaration on the Principles of International Law made the exchange clearer still when it included *the principle concerning the duty not to intervene in matters within the domestic jurisdiction of any State*, set out in the following terms:

- No state or group of states has the right to intervene, directly or indirectly, for any reason whatever, in the internal or external affairs of any other State.

[7] R. Falk, 'Sovereignty', *Oxford Companion to Politics of the World* (OUP, 1993), p.853.

- No state may use or encourage the use of economic, political or any other type of measures to coerce another state in order to obtain from it the subordination of the exercise of its sovereign rights and to secure from it advantages of any kind.
- Every state has an inalienable right to choose its political, economic, social and cultural systems, without interference in any form by another state.[8]

The Work of the UN Groups of Governmental Experts

The necessary relationship between sovereignty and non-intervention resonates loudly in the context of international security in cyberspace. The three sets of responsibilities outlined earlier are all reflected in the 2013 and 2015 GGE reports, notably in their references to the UN Charter.

The UN GGE reports include several references to questions of sovereignty, which in turn imply responsibilities on the part of the state with regard to other states and the international community. The principle of 'responsibility' also finds expression in customary international law and is manifested most clearly in the law of state responsibility.[9] In this regard, the international law section of the 2015 report includes specific references to the (peacetime) responsibility of states to i) meet their international obligations regarding internationally wrongful acts attributable to them under international law (para. 28 f); and ii) not to use proxies to commit internationally wrongful acts and to prevent their territory from being used by non-state actors to commit such acts (para. 28 e).[10] The report also includes references to the obligations of states with regards to human rights and international humanitarian law.[11]

In addition to its focus on international law, the 2015 GGE report considered the role of non-binding norms in shaping the responsible behaviour of states, noting that:

> Voluntary, non-binding norms of responsible State behaviour can reduce risks to international peace, security and stability. Accordingly, norms do not seek to limit or prohibit action that is otherwise consistent with international law. Norms reflect the expectations of the international community, set standards for responsible State behaviour and allow the international community to assess the activities and intentions of States. Norms can help to prevent conflict in the ICT environment and contribute to its peaceful use to enable the full realization of ICTs to increase global social and economic development.

The GGE thus recommended a number of non-binding norms (eleven in total) of responsible behaviour of states aimed at promoting an open, secure, stable, accessible and peaceful ICT environment.[12] The UN General Assembly subsequently called upon UN member states "to be guided in their use of information and communications technologies by the 2015 report of the Group of Governmental Experts".

The norms are a mix of restraint measures and positive duties relating to co-operation, attribution, the protection and resilience of the critical (information) infrastructure and the global ICT infrastructure, protection of civilians, countering the spread of malicious ICT tools and techniques, integrity of the supply chain, vulnerability disclosure and the sharing of information, and the protection of CERTs and CSIRTs, as follows:

---

[8] *Declaration on Principles of International Law Concerning Friendly Relations and Co-operation Among States in Accordance with the Charter of the United Nations* (General Assembly Resolution 2625 (XXV), 1970), in M.D. Evans (ed.), *Blackstone's International Law Documents* (London: Blackstone, 1996 [3rd edition], p.209.

[9] For a discussion on the links between cybersecurity and due diligence, see: S.J. Shackelford, S. Russell and A. Kuehn, 'Unpacking the International Law on Cybersecurity Due Diligence: Lessons from the Public and Private Sectors', *Chicago Journal of International Law* (Vol. 17, No. 1, Article 1, 2016). Available at: http://chicagounbound.uchicago.edu/cjil/vol17/iss1/1

[10] As noted by Jason Jolley, the law of state responsibility can broadly be explained by its two underlying principles: states can be held responsible for acts that are attributable to them and states can only be held responsible for internationally wrongful acts, that is, for breaches of their obligations towards other states. J. Jolley, *Attribution, state responsibility, and the duty to prevent malicious cyber-attacks international law* (University of Glasgow, PhD thesis, 2017), p.69: http://theses.gla.ac.uk/8452/1/2017JolleyPhD.pdf

[11] UN General Assembly, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (UNGA: A/70/174, 22 July 2015). Available at: http://undocs.org/A/70/174

[12] Ibid, pp.7-8.

a) Consistent with the purposes of the United Nations, including to maintain international peace and security, States should cooperate in developing and applying measures to increase stability and security in the use of ICTs and to prevent ICT practices that are acknowledged to be harmful or that may pose threats to international peace and security;
b) In case of ICT incidents, States should consider all relevant information, including the larger context of the event, the challenges of attribution in the ICT environment and the nature and extent of the consequences;
c) States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs;
d) States should consider how best to cooperate to exchange information, assist each other, prosecute terrorist and criminal use of ICTs and implement other cooperative measures to address such threats. States may need to consider whether new measures need to be developed in this respect;
e) States, in ensuring the secure use of ICTs, should respect Human Rights Council resolutions 20/8 and 26/13 on the promotion, protection and enjoyment of human rights on the Internet, as well as General Assembly resolutions 68/167 and 69/166 on the right to privacy in the digital age, to guarantee full respect for human rights, including the right to freedom of expression;
f) A State should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public;
g) States should take appropriate measures to protect their critical infrastructure from ICT threats, taking into account General Assembly resolution 58/199 on the creation of a global culture of cybersecurity and the protection of critical information infrastructures, and other relevant resolutions;
h) States should respond to appropriate requests for assistance by another State whose critical infrastructure is subject to malicious ICT acts. States should also respond to appropriate requests to mitigate malicious ICT activity aimed at the critical infrastructure of another State emanating from their territory, taking into account due regard for sovereignty;
i) States should take reasonable steps to ensure the integrity of the supply chain so that end users can have confidence in the security of ICT products. States should seek to prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions;
j) States should encourage responsible reporting of ICT vulnerabilities and share associated information on available remedies to such vulnerabilities to limit and possibly eliminate potential threats to ICTs and ICT-dependent infrastructure;
k) States should not conduct or knowingly support activity to harm the information systems of the authorized emergency response teams (sometimes known as computer emergency response teams or cybersecurity incident response teams) of another State. A State should not use authorized emergency response teams to engage in malicious international activity.

As noted above, some of these norms derive from existing principles of international law and can be said to be aimed at preventing harm. For instance, paragraph 13 c) of the 2015 report relates to the principle of due diligence and state responsibility. The norm recommending that "States should not knowingly allow their territory to be used for internationally wrongful acts" provides links to the international law section and is argued by Liisi Adamson to provide "a baseline for state accountability in instances where transboundary harm emanates from its territory".[13] Similarly, the norm recommending that States "should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public"[14] draws from the basic construct of state responsibility.

Both norms referred to above are strongly linked to many of the other recommended norms, as well as the recommended cooperative, confidence and capacity building measures. Nonetheless, their placement in the non-binding norms section of the GGE report arguably reflects divergences among states on the law of state responsibility and the principle of due diligence. Those who view state responsibility as legally binding generally refer to the Draft Articles on the Responsibility of States for Internationally Wrongful Acts (Draft Articles), viewing the International Law Commission's codification of the articles as reflective of customary international law. Following four decades of

[13] L. Adamson, 'Recommendation 13(c)' in UNODA, *Voluntary, Non-Binding Norms for Responsible State Behaviour in the Use of Information and Communications Technology: A Commentary* (New York: United Nations, 2017), p.51.
[14] UN GGE 2015, para. 13 (f).

codification, the rules of the Draft Articles have since been endorsed by the General Assembly and are considered a highly authoritative source of soft law which states are generally expected to follow.[15]

Not all states agree, however, on the legal status of the Draft Articles. The outstanding question for the Geneva Dialogue is not to assess the legal merit of the GGE norms, however, but to understand how the norms might best be operationalized or implemented as a means to contribute to international security and stability. Operationalizing the norms can also help identify if additional norms are required as well as obstacles to implementation such as resource and capacity gaps.

Several of the norms recommended in 2015 relate to critical infrastructure. It is often argued, even if only metaphorically, that while the government of a state carries 90 percent (or thereabouts) of the responsibility for the *security* of critical national infrastructure, in many cases the private sector is responsible for the *ownership* or *management* of a similar proportion of it. Where the critical information infrastructure is concerned, this imbalance of responsibility is often further complicated by the crossborder ownership and management of infrastructure providers. We thus have a second dimension to the transactional nature of state responsibility – this time involving the private sector. There must, self-evidently, be a shared or pooled responsibility arrangement between public and private sectors in which the state surrenders some of its traditional responsibility for the protection of sovereign territory, property, interests etc, while the private sector accepts some aspects of a public role. Indeed, this is a critically important responsibility to be undertaken by states acting in concert with the private sector internationally. Understanding how this engagement on critical infrastructure is playing out in practice and sharing experiences would be an excellent contribution by the Geneva Dialogue to upcoming processes such as the Open-Ended Working Group and the UN GGE. Furthermore, in the current international environment which has seen a growing entanglement of global companies in traditional geopolitics, the question of how responsible behaviour can be pooled or shared more effectively remains critical.

In exercising responsible behaviour, states also need to adapt existing risk assessment methodologies to take into account the vulnerability to harm in/from cyberspace and, relatedly, the systemic significance of technical risk (vulnerabilities in software and hardware, the possibility that the supply chain might be interfered with etc.). The latter point relates specifically to the norm (GGE 2015 13(i)) encouraging states 'to prevent the proliferation of malicious ICT tools and techniques', creating the expectation that states should encourage a shared responsibility of the technology sector. It follows that states should assess whether initiatives such as vulnerability equity processes and coordinated vulnerability disclosure, or using existing technology transfer control mechanisms such as the (non-legally binding) Wassenaar Arrangement, to deal with proliferation of malicious ICT tools and techniques can be effective without dealing with the fundamental systemic problems haunting the global ICT industry. Again, the Geneva Dialogue can serve as a platform for States to share experiences and practices of their efforts to deal with systemic technological vulnerabilities.

States also need to find ways to prevent conflict arising from the malicious use of these technologies, from the potential for misunderstanding and miscalculation arising from the growing reliance on offensive cyber capacity or triggered by technological vulnerabilities or basic human error. To this end, the UN GGE reports recommended a number of confidence building and cooperative measures. These have since been taken up by regional organisations such as the Organisation for Security and Cooperation in Europe (OSCE), the ASEAN Regional Forum (ARF) and the Organisation for American States (OAS) One open question for the Geneva Dialogue is whether the measures that have been adopted to date by regional organisations are sufficient in this respect. Equally, it remains

[15] Once completed, the UN General Assembly commended the Articles to governments. GA Res. 56/83, UN Doc. A/RES/ 56/83 (12 December 2001). By 2012, the Articles and the accompanying commentary had been cited 154 times by international courts, tribunals, and other bodies. United Nations Materials on the Responsibility of States for Internationally Wrongful Acts, UN Doc. ST/LEG/SER B/25 (2012). Referenced in M. Schmitt (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge: Cambridge University Press, 2017).

to be seen whether states have established sufficiently robust mechanisms to manage and resolve crises as they develop: a number of Track 1.5 and 2.0 initiatives have been pursued to this end but their efficacy is unclear.

Complementary Expectations

Policy and strategy development

States are expected to communicate their intentions to a new range of actors, using different mechanisms such as a national cyber/digital security strategy, of the sort being developed by an increasing number of states. The development and implementation of such strategies also implies the engagement of other actors at national level, including with regard to civilian oversight. Some policies and strategies are straightforward and largely speak to a longer-term vision of maturity and protection against harm, and protection of national interests. Others are anchored in doctrinal concepts such as mutual deterrence, arguably one of the most significant legacies of Cold War inter-state politics. However, the adaptation of deterrence thinking from Cold War circumstances has not proved to be straightforward, although the expert debate on the subject remains nonetheless very active. Since the goal of deterrence is the avoidance of conflict, it is clear that some states view deterrence (whether unilateral or mutual) as a component of state responsibility. The US in particular, has embraced the concept "to deter destabilizing state conduct in cyberspace" both above and below the threshold of armed conflict.[16] For its part, the EU has launched a 'Cyber Diplomacy Toolbox', to "develop signalling and reactive capacities at an EU and member state level" to influence the behaviour of potential aggressors.[17] Deterrence measures are often critiqued for the reciprocal reaction they provoke (the basis of a security dilemma) and the concept is contested by numerous states who perceive it as a justification for 'militarizing' the ICT environment.

Cross-border collaboration

The effective exercise of responsible behaviour also requires cross-border collaboration, another point raised in the successive GGE reports. At the operational level, this can require reliance on existing bilateral or multilateral agreements on jurisdictional authority and on enforcement mechanisms and identification of possible gaps in these instruments and mechanisms.

Capacity building and technical cooperation

Capacity-building is necessary in any area of public policy where government assesses that it lacks the means to achieve its policy goals. It follows that before embarking upon a systematic capacity-building programme, government must first establish what those goals might be. Without clear purpose, capacity-building will be an aimless activity and government will be unable to prioritise among alternative demands for the use of official time and public funds. Where cyber security is concerned, government might require a range of capacity-building options from which to select the optimal cost/benefit combination in the circumstances it confronts. The latter point is critical: even though cyber security is still in an immature state as far as politico-diplomatic relations are concerned, governments must nevertheless situate their capacity-building ambitions in the context of potential ICT-related conflict as far as it can be determined. This becomes particularly important where cyber security capacity-building is being undertaken by developing countries. The importance of cyber security capacity building was recognised in the GGE reports and over the past decade, a whole industry has emerged around it.

Technical co-operation between and among national authorities is a clear indicator of the possibility of stronger and more ambitious preventive diplomacy where ICT-related conflict is concerned. Information-exchange (including vulnerability disclosure) and alert-sharing agreements between Computer Emergency Response Teams (CERTs) and Computer Security Incident Response Teams

[16] See US Department of State, 'Recommendations to the President on Deterring Adversaries and Better Protecting the American People From Cyber Threats', 18 May 2018: https://www.state.gov/s/cyberissues/eo13800/282011.htm

[17] E. Moret and P. Pawlak, 'The EU Cyber Diplomacy Toolbox: towards a cyber sanctions regime?', *EUISS Issue Brief* (24, July 2017), p.1.

(CSIRTs) can help to establish a relationship of trust between governments, relationships which can be particularly valuable when governments are exposed to ICT-related aggression of some sort.

Key Points from the Geneva Dialogue Workshop relating to the Roles and Responsibilities of States

The discussion of the roles and responsibilities of states in cyberspace in the context of international security and stability can be summarised as follows:

- States respond in different ways to the risks and opportunities of cyberspace: some are averse to confrontation and malicious activity while others see cyberspace as an opportunity to undertake (or encourage) destabilising and criminal acts from which they expect to benefit in some political, strategic or economic way; a third category of states seek to occupy both behavioural categories – the 'responsible actor and the 'outlaw' – simultaneously. At present the international system lacks the means with which to insist upon, and enforce, agreed standards of responsible behaviour.
- The risk of breakdown is heightening. The variety, level and complexity of destabilising and malicious behaviours increase, while mitigating agreements and procedures continue to evolve at a slower pace: it is no exaggeration to conclude that international peace and security could be endangered, either deliberately through the acquisition and use of offensive cyber means, persistent subversive activity aimed at undermining or influencing political processes such as elections, or as the result of diplomatic misunderstanding or strategic miscalculation.
- Expectations of responsible behaviour by states are long-established and are clear (if not entirely uncontested) in international law. The UNGGE has made important progress in translating these expectations into the ICT context, in the form of a set of eleven non-binding norms of responsible state behaviour. However, some states appear to take the view that they can ignore these expectations – as well as international law itself – if they consider it to be in their sovereign interests to do so. If the UNGGE norms are to be operationalised and implemented, the obvious challenge is to persuade states that responsible behaviour is the necessary, and mutually beneficial counterpart to state sovereignty rather than an optional addition to it.
- There are certain areas in which the benefits of mutual, self-reinforcing responsible behaviour are clear. For example, working with the private sector to ensure the resilience of critical national and cross-border ICT (or ICT-based) infrastructure, or participation in confidence building and dialogue processes in order to minimise the risk of diplomatic misunderstanding and strategic miscalculation, and manage crisis.

SECTION 3: SHARING RESPONSIBILITY IN CYBERSPACE

The Geneva Dialogue on Responsible Behaviour in Cyberspace is concerned with analysing the roles and responsibilities not only of states, but also of "industry actors and civil society, academic and tech communities" in contributing jointly to "greater security and stability in cyberspace".[18] This section of the report discusses the roles and responsibilities of this broad range of actors, examining the relationships between these actors, their relationships with states and, in particular, their knowledge of, and interaction with the norms set out by the UN Group of Governmental Experts. From the perspective of the Geneva Dialogue, the different actors in this category exercise responsible behaviour in cyberspace in a number of different ways. These might best be described as **'reactive'**, or '**productive**' behaviours.[19] Sometimes both are exercised simultaneously. The first category, **'reactive behaviours'**, are generally articulated or deployed in response to, or in anticipation of the behaviours of states or other actors, particularly when they violate – or risk violating – existing norms and principles. The second category - '**productive behaviours'** – refer to those behaviours that contribute or respond to changes in the technological and normative landscape, thus influencing the landscapes, their own behaviours and those of others.

In an obvious way, the ambition of the Geneva Dialogue corresponds precisely with the structure and character of cyberspace, particularly the Internet. The Internet is used and valued by a vast range of users and stakeholders and on every level imaginable – from the private individual up to the largest corporate entities. What is more, co-operation between these different stakeholders, and across the many different levels and sectors of activity is structurally necessary to the functioning and the perceived value of the Internet. To use a much over-used metaphor, it might even be said that complex co-operation of this sort is 'in the DNA' of the Internet and broader cyberspace. But the Internet is shaped not just by the *quantity* of its users and the volume of data and information being distributed: 'complex co-operation' is also a *qualitative* phenomenon. This is most clearly the case when we consider how best to achieve greater security and stability in cyberspace.

In the modern era, the maintenance of international peace and security (and, indeed, its opposite) has been generally considered to be the responsibility of the sovereign state. In the era of the Internet and growing technological dependence, this expectation largely still obtains. Yet an important shift has taken place at the practical level. In the past we might have assumed that states would co-opt and orchestrate the various components of national power (diplomatic, industrial, military, economic) in order to ensure security and stability. In the technological era, however, many of the most influential sources of 'power' in the international system do not consider themselves to be answerable, let alone responsible to states. Technology sector companies, for example, as well as human rights and privacy advocacy groups, might on principle be reluctant to be co-opted into a state-led security and stability effort, no matter what its merits. Yet it is hard to imagine that the security and stability of cyberspace could be achieved – or could endure for long – without the active involvement of these different sources of both 'hard' and 'soft' power. Thus, just as the operation of the Internet requires 'complex co-operation', so the pursuit of security and stability in this environment will require something similar. States will continue to do what only they can do, in respect of diplomatic and economic interaction, intelligence gathering and, in the last resort, the use of coercive force of some sort. But rather than seek to *orchestrate* these new sources of 'cyber power' under national leadership, states must instead seek to *co-operate* with these other actors; respecting not only that these actors have certain types of competence (and, consequently, authority) in cyberspace which states generally do not have, but also that the independence of these actors is critical to the functioning of cyberspace.

[18] Geneva Dialogue website: : https://genevadialogue.ch/and https://www.giplatform.org/events/geneva-dialogue-responsible-behaviour-cyberspace

[19] The authors are grateful to Dennis Broeders, Director of the Norms initiative at Leiden University for his insights on this topic.

Private Sector and Industry Actors

Background

Where international peace and security is concerned, it has not been unusual for industrial concerns and other private sector bodies to be closely involved with government agencies and departments, in a wide array of circumstances and often at high intensity. At the military operational level, in almost 30 years since the end of the Cold War it has been increasingly common for civilian defence contractors to deploy alongside their military clients in armed interventions of various sorts. This relationship has in turn led to the emergence of new norms. At the highest levels of international diplomacy, the private/technology sector has a long history of '**reactive behaviours'**, contributing, for instance, to the structure and design of multilateral technology transfer control lists, covering a wide range of specialised and/or dual-use technologies, control of which is considered to be essential to the maintenance of international peace and security. And in the highly evolved sphere of arms control and disarmament, the chemical industry was very closely involved in devising the inspection and verification regime of the Organisation for the Prohibition of Chemical Weapons, established in 1997.

The private sector has also, of course, been heavily engaged in promoting '**productive behaviours'**. Indeed, parts of the private sector have been central to the development and diffusion of ICT around the world in recent decades, driven in large part by the privatisation of the Internet in the late nineties. In this regard, a large part of the private sector's contribution has been in the development and steady supply of products and services, such that private sector stakeholders are generally recognised for having made important contributions to the "international […] architecture for the governance of cyberspace."[20] The fact that this architecture is highly vulnerable means that certain technology sector actors are viewed as bearing significant responsibility. In the increasingly urgent, practical matter of ensuring the security, functionality and stability of cyberspace, the role of the private sector has become nothing short of critical.

Extant Roles and Responsibilities

Given its focus on international security and stability, the Geneva Dialogue is especially interested in those private sector actors whose reactive and productive behaviours (or a combination of both) contribute to the **resilience** of critical national and transnational infrastructure (particularly with regards to critical information infrastructure and the finance, and energy sectors, but also including the integrity and resilience of democratic electoral systems); in guaranteeing persistent levels of **service** (i.e. business continuity planning and preparation); and in ensuring the **security and integrity of the ICT supply chain**. In the highly technical environment that is cyberspace, there are several other areas of activity which, although traditionally assumed to be the responsibility of state authorities, are also areas in which state capacity is often lacking or at worst completely absent, and in which the private sector is increasingly expected to play a role: the detection of cyber-dependent or cyber-enabled **crime** (including the *criminal proxy* dimension); the detection of **subversive activity** by one state against another; and, in the political-military and intelligence spheres, technical assistance in **attribution**, **cyber-defence**, **cyber-deterrence** and **operational response**. For the purpose of this first phase of the Geneva Dialogue, the focus has been largely on actors in the IT industry, who are key to many of the functions listed above.

This list of security-related activities is impressive, not only for the wide variety of ways in which the private sector might contribute, but also because the private sector is clearly expected to have a more instrumental (rather than simply advisory or auxiliary) role in what has traditionally been considered to be the core business of the state – security and defence. On this evidence, it would seem that a shift in political, and even constitutional responsibilities is taking place. Evidence of this shift can also be found in the increase in reactive-productive behaviours on the part of the private sector, i.e. the

[20] R. Radu, 'Power Technology and Powerful Technologies: Global Governmentality and Security in the Cyberspace' in J.-F. Kremer and B. Müller (eds), *Cyberspace and International Relations: Theory, Prospects and Challenges* (Berlin and Heidelberg: Springer-Verlag, 2014), p.4.

tendency of industry and technology sector companies or bodies to act as so-called 'norm entrepreneurs'. As owners and managers of large parts of critical network infrastructures and technology platforms, they have come to wield considerable influence over key aspects of cyberspace and human existence: "Internet companies have become central platforms for discussion and debate, information access, commerce and human development. They collect and retain the personal data of billions of individuals, including information about their habits, whereabouts and activities, and often claim civic roles."[21] Just as the involvement of the private sector in national and international cyber security and stability invites (if not necessitates) critical assessment, so the claim to 'civic roles' should demand closer inspection.

Private sector actors have developed a distinctive approach to the 'roles and responsibilities' debate, largely in the context of self-regulation initiatives. These initiatives, of clear relevance for the Geneva Dialogue, include **norm development** and **promotion** with regard to state and industry behaviours; **awareness-raising** on threats and protection methods among technology developer and end-user communities; **capacity building** in the private sector and among the general public through education and engagement in public-private partnerships; **information** exchange and the sharing of **best practice**; the development of industry/sectoral norms through **standardisation** e.g. in software assurance and secure development practices and in agreeing standards for **'privacy by default and security by design'**; and initiatives in **transparency** and **vulnerability/breach notification**.

Self-regulation, however, is not quite the same thing as state regulation, and it would be reasonable to ask what motivates private sector bodies to become more involved in taking on these ostensibly civic roles. This is not to cast gratuitous suspicion on initiatives such as Siemens' 'Charter of Trust', Microsoft's 'Digital Peace Now' initiative and its advocacy of norms of responsible State and industry behaviour (culminating ideally – for Microsoft – in a 'Digital Geneva Convention'), the multiple-signatory Cybersecurity Tech Accord, Google's 'Project Zero', Kaspersky's 'Global Transparency Initiative, and Telefonica's Manifesto for a New Digital Deal', all of which appear to be admirable efforts to promote high standards of self-regulation and responsible behaviour within the private sector. After all, it would be perverse to insist, in one moment, that the private sector should be more involved in the security and stability of cyberspace, nationally and internationally, and then, in the next moment, to reject these initiatives on suspicion that they must be merely self-serving. Yet a genuine partnership between the public and private sectors must be mutually beneficial and must be seen as such; the civic space, and the normative framework underpinning it, are critically important features of liberal democratic society, requiring protection in the form of governance, oversight and accountability.

The case for a (constructively) critical response to these private sector initiatives is emphasised by the fact that some private sector actors, while being active developers and implementers of security technology and procedures, have at the same time also produced or contributed to heightened levels of *in*security. By speeding up product development lifecycles, releasing insecure products to the market and failing to update and maintain legacy systems, some companies have furthered the prevalence of systemic vulnerabilities.[22] Moreover, as part of their protective measures, some enterprises have engaged in what can only be described, in language usually associated with governments and ministries of defence, as 'offensive cyber operations', arguing that states are lacking the necessary capacity to adequately defend their interests and safeguard their existence. Such practices, however, including hack-backs, are arguably *not* conducive to international cyber security

[21] United Nations Human Rights Council, 'Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression' (2018) para. 9: https://documents-dds-ny.un.org/doc/UNDOC/GEN/G18/096/72/PDF/G1809672.pdf?OpenElement

[22] Although the development of fully secure software of nontrivial size and complexity is illusory, premature software releases to meet customer demand without adequate care for security introduce considerable dangers. See The New Republic, 'U.S. Cybersecurity: Why Is Software So Insecure?' (11 October 2013): https://newrepublic.com/article/115145/us-cybersecurity-why-software-so-insecure

and stability. Not only do they have the potential to result in serious disruption and harm, but they are also likely to increase the chances for escalation and fallout.[23]

Key Points from the Geneva Dialogue Workshop relating to the Private Sector

Interaction with the UN GGE Recommendations:

- Experts at the Geneva Dialogue workshop noted how many of the reactive and productive behaviours discussed in the preceding paragraphs respond in important ways to calls for private sector engagement included in the UN GGE reports of 2010, 2013, and 2015.[24] These make reference to the importance of engaging private actors in cooperative and confidence building measures, ICT security and capacity building assistance, public-private partnerships, and exchanges of information between CERTs and within and beyond CERT communities. Paragraph 31 of the 2015 The UN GGE 2015 report, for example, holds that "while States have a primary responsibility for maintaining a secure and peaceful ICT environment, effective international cooperation would benefit from identifying mechanisms for the participation, as appropriate, of the private sector, academia and civil society organizations."[25]

- The provisional Table in Annex 1[26] identifies those norms around which participants at the first workshop of the Geneva Dialogue believe private sector actors already contribute through their own work, or where greater interaction can be fostered in support of their implementation. At the same time, while there appears to be a general recognition, particularly among Western stakeholders, that engagement with the private sector is key to implementing many of the recommendations of the UN GGE, the roles and responsibilities of private sector entities remain unclear and require further consideration.

- Initiatives such as the recent Paris Call for Trust and Security in Cyberspace, the Siemens Charter of Trust, the Cybersecurity Tech Accord, the Digital Peace Now campaign and Kaspersky's Transparency initiative were all discussed as examples of self-regulatory initiatives promoted by the technology sector and which complement the work of the UN GGEs. A next step for the Geneva Dialogue would be to discuss how the results/impact of these corporate initiatives are collected, assessed and published and how companies can better engage their peers and supply chains, as well as the public in general, in such initiatives.

- A discussion on existing and emerging norms relating to ensuring that private companies refrain from backing or providing services to sovereign entities in acts of subversion and offensive action is also key.

Other outstanding issues:

- There is a serious disjunction between micro-level and macro-level efforts to deal with technological vulnerabilities. A key focus of the Geneva Dialogue moving forward should be to assess ongoing efforts such as national and international Vulnerability Equity Processes and

[23] Hack-back refers to a type of active cyber defence conducted by a victim (on a perpetrator's infrastructure), in reaction to an initial attack, and with the intention of inflicting repercussive harm or gaining retribution.

[24] United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 'Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security' (UN GGE 2010): http://www.un.org/ga/search/view_doc.asp?symbol=A/65/201; United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 'Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security' (UN GGE 2013): http://www.un.org/ga/search/view_doc.asp?symbol=A/68/98; UN GGE 2015: http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174

[25] UN GGE 2015, para. 31.

[26] The Table at Annex 1 is PROVISIONAL. The table includes illustrations and examples discussed during the civil society and private sector breakout groups at a workshop in Geneva in November 2018. The authors suggest further, systematic development of the table, possibly in conjunction with an external norms-related initiative.

Coordinated Vulnerability Disclosure initiatives,[27] and identify other approaches involving the technology sector that address vulnerability challenges and associated risks.

- Participants at the Geneva Dialogue workshop agreed that industry representatives have a key responsibility for providing adequate levels of security to customers of relevant products and services, in direct user protection, in assisting with the attribution of, and response to cyber incidents as well as in raising resilience levels. A next phase of the Geneva Dialogue should focus on identifying good practices in this regard.

- There is a growing climate of mutual distrust and uncertainty between private and public sector entities. To better understand the respective roles of governments and corporations and help foster trust and credibility, it will be important to develop scalable frameworks of interaction and collaboration. Existing institutional structures such as the Global Forum for Cyber Expertise and the London process were discussed as important platforms for such interaction and cooperation.

- Representatives from sectors other than the technology sector should be brought into the Geneva Dialogue and should necessarily include representatives from the financial, energy and insurance sectors.

Civil Society and other Key Actors

Background

Other key actors in the discussion of responsible behaviour in cyberspace include non-governmental organisations, policy research institutions, academia, and expert communities such as the technical community that occupy what is often referred to as the 'civil society sphere'. The participation of many of these actors in the international peace and security sphere is not new and there are extensive examples of areas in which states have accommodated such engagement. A very current and notable example is the participation of a variety of different actors in the UN Conference on Disarmament's continuing discussions on lethal autonomous weapons (LAWs). Today, these different actors are broadly considered central to the achievement of an open, secure, stable, accessible and peaceful cyberspace.

As noted elsewhere, the very nature of cyberspace, the broad range of normative concerns involved, and the range of behaviours that pose risks to the maintenance of international peace and security call for much deeper – and possibly more responsible – civil society engagement than experienced in other areas. Such engagement can afford greater legitimacy and sustainability to on-going multi-lateral processes concerning international security and ICT. It can also help ensure that normative concerns are attended to, and that the right technical expertise is leveraged when solutions are sought.[28] Moreover, many of these 'other actors' are often victims of the behaviours of other actors online, thus giving them even more reason to engage.

Based on practice across other international security agendas such as arms control and disarmament, these different actors engage and exercise responsibility in cyberspace in a range of different ways. For instance, academic experts or representatives from think-tanks, technical communities or civil society organisations contribute analytically to identifying and classifying threats and actively engage in proposing solutions to manage risk. They inform government thinking and position development ahead of negotiations. Sometimes they participate in multilateral processes independently as experts, or as part of government delegations (although these options evidently depend on government receptivity to such forms of engagement). They participate in or demand hearings before and after

[27] See, for example, the Global Forum on Cyber Expertise, *Co-ordinated Vulnerability Disclosure*, November 2017: https://www.thegfce.com/initiatives/r/responsible-disclosure-initiative-ethical-hacking

[28] C. Kavanagh and D. Stauffacher, 'A Role for Civil Society' (ICT4Peace Foundation, 2014): https://ict4peace.org/wp-content/uploads/2014/09/processbrief_2014_II_draft6_2.pdf

government participation in multi-lateral processes and can promote adherence to and implementation of policy outcomes. For instance, the International Campaign to Abolish Nuclear Weapons (ICAN), a coalition of non-governmental organizations, has been instrumental in promoting adherence to and implementation of the United Nations nuclear weapon ban treaty. They also organise and coordinate their own actions on specific agendas through thematic networks or issue-specific platforms.

Extant Roles and Responsibilities

From the perspective of the Geneva Dialogue, the different actors in this category exercise responsible behaviour in cyberspace in a number of different ways. As with private sector actors, these might best be described as '**reactive**', or '**productive**' behaviours or a mix of both.[29] As discussed, the first category, 'reactive behaviours', are generally articulated or deployed in response to or in anticipation of the behaviours of States or private sector actors, particularly when they violate – or risk violating - existing norms and principles. These behaviours are reflected in on-going **advocacy, awareness raising and oversight** work on human rights, privacy and accountability issues, and are often accompanied by research in the technical, legal and sociology fields. They specifically involve monitoring and publicising state and corporate practices that negatively impact civil society. Indeed, civil society groups are often the targets of malicious activities by states or state-supported actors. because they often lack the capacity or knowledge to identify and counter them.[30] They can also serve as early warning mechanisms for emerging threats[31]. The work of groups such as the Citizen Lab, the Institute of Electrical and Electronics Engineers (IEEE), AccessNow, the ICT4 Peace Foundation, Human Rights Watch, GlobalPartners and numerous cross-disciplinary university centres has been fundamental in this regard. Some suggest the need to broaden this group of actors to include consumer protection associations.

Such 'reactive' behaviours are also evident in targeted research (on emerging threats, cyber conflict, crisis management, deterrence, attribution and norms). They are also evident in semi-formal and informal **diplomacy** efforts such as track 1.5 and track 2 dialogues involving or hosted by think-tanks or academic groups. In this case, these actors respond to the absence of - or deadlock in - formal diplomatic channels or provide discrete (and plausibly deniable) venues for building confidence, facilitating exchanges on sensitive issues relating to doctrine and strategy. In the context of international peace and security, the overarching objective of such track 2 and 1.5 dialogues is to establish a basis to for managing crisis in the event of an escalation of tensions. Current and past examples include the MIT Roundtable on Military Cyber Stability; and the US-China, UK-China, Sino-European and US-Russia dialogues.

Other responsible behaviours attributed to these different actors might be termed as '**productive behaviours'** in that in that they are constantly contributing and responding to changes in the technological and normative landscape and in doing so influence the landscapes, their own behaviours and those of others. This is particularly the case for members of the co-called 'technology' community whose combined work contributes to the functioning of the Internet, in turn fundamental for an open, accessible, secure and stable ICT environment. The incident response work of CERTs and CSIRTs is another important example of such productive responsibilities. Other 'productive' behaviours would include **awareness raising, capacity building** and **exchanges of knowledge** and **expertise** on technical issues, policy, doctrine and strategy; longer-term state building elements such as education curricula (primary, secondary and tertiary); norm shaping and related efforts on standards, regulation and national legal frameworks; and efforts to ensure civilian oversight and influence budgetary frameworks. Some of these efforts are considered in the work of the platforms such as the Global

[29] The authors are grateful to Dennis Broeders, Director of the Norms initiative at Leiden University for his insights on this topic.
[30] The University of Toronto's Citizen Lab has been particularly vocal about threats directed against non-government, non-military targets. See: https://citizenlab.ca/
[31] OSCE, 'The Role of Civil Society in Preventing and Countering Violent Extremism and Radicalization that Lead to Terrorism: A Focus on South-Eastern Europe' (18 October 2018): https://www.osce.org/secretariat/400241

Forum on Cyber Expertise (GFCE) and its respective members;[32] the Geneva Internet Platform (GIP) Digital Watch observatory[33] or more targeted initiatives such as the ICT4Peace Foundation's International Cyber Security Capacity Building Workshops.[34]

Other forms of productive behaviours include **academic** and **applied research**, including that which covers (or straddles) computer and engineering studies, technical security research, international law, international relations, international security and strategic studies, social and behavioural sciences. Adding to the value they bring to discussions on international peace and security, civil society groups commonly share extensive knowledge and experience in developing more long-term programmes that promote peace and dialogue. Usually well-versed in local dynamics and trends, they have the legitimacy and influence to address concerns at 'grass roots' levels and their connectedness facilitates work across nations, communities and disciplines.

Key Points from the Geneva Dialogue Workshop relating to Civil Society

Interaction with the UN GGE Recommendations:

- Governments have for some time articulated that they alone cannot address the nature and volume of risks associated with interconnected networks and our growing reliance on information technologies. While still bearing primary responsibility for national security and the safety of citizens, including in the ICT environment,[35] they have stressed the importance of engaging civil society actors in processes relating to ICT and international peace and security. The first GGE report in 2010 acknowledged that confronting the challenges of the twenty-first century depends not only on cooperation between States but also on collaboration and cooperation between States and other actors such as civil society (and the private sector) and recommended the exploration of cooperative actions and mechanisms to that effect.

- Furthermore, some of the 'reactive' and 'productive' behaviours discussed above are specifically acknowledged in the reports. For example, the 2013 report reiterated the point made in the 2010 report on the importance of cooperation and collaboration with other actors, although it also acknowledged that the work of states in developing confidence building measures would benefit from the involvement of civil society (and the private sector). This specific reference to the value of engaging other actors in State-led CBMs also appears in the context of the first set of OSCE CBMs developed to reduce the risk of conflict stemming from the use of ICT.[36] This reflects the guidance put forward in the OSCE guide on non-military CBMs, which stresses the importance of civil society participation, particularly regarding CBM implementation. A 2014 OSCE Chairmanship Event subsequently recommended that non-state stakeholders be offered a platform to engage in state-centric processes through the "promotion of regular academic feedback" such as annual exchanges and special meetings.[37] The 2013 GGE report also highlighted the importance of incident response capabilities and the need to strengthen CERT-to-CERT cooperation (many CERTs would argue that this was already underway, independent of state involvement).

[32] GFCE: https://www.thegfce.com/
[33] The GIP provides information on international developments and actors related to cyber security-related policy areas. Its range of topics makes it a "one-stop shop" for overviews of relevant issues, events, actors, instruments and processes, including explanations and live updates: https://dig.watch/
[34] ICT4Peace, 'International Cyber Security Capacity Building Workshops. Promoting Openness, Prosperity, Trust and Security in Cyberspace' (2014): http://ict4peace.org/wp-content/uploads/2017/10/Outline-Capacity-Building-2017811.pdf
[35] UN GGE 2015, para. 19.
[36] CBM 7 specifies that "participating states will voluntarily share information on their national organization; strategies; policies and programmes – including on co-operation between the public and the private sector". Add reference
[37] OSCE Chairmanship Event Summary, CIO.GAL/238/14, 22 December 2014: https://www.giplatform.org/sites/default/files/Summary%20Chairmanship%20in%20Office%20Event.pdf For an assessment of efforts by regional organisations to develop the role of civil society and academic organisations see DiploFoundation, *Towards a Secure Cyberspace via Regional Co-operation* (2017), p.16: https://www.diplomacy.edu//sites/default/files/Diplo-Towards_a_secure_cyberspace-GGE.pdf

- The 2015 report again acknowledged that international cooperation would benefit from the 'participation' of other actors beyond states – this time adding academia – and encouraged the identification of mechanisms to enable such participation, particularly with regard to "ICT security capacity building" for "improv[ing] the environment for effective mutual assistance between States in their response to ICT incidents".[38] The same GGE report strengthened the reference to CERTs, noting the importance of bilateral exchanges of information and communication and within CERT communities and other fora as a means "to support dialogue at political and policy levels". The report also recommended that "think tanks and research organisations" could be requested to undertake "further research and study, including on concepts relevant to State uses of ICT". To date, it has been hard to identify systematically how these recommendations have been followed through, although initiatives such as the GFCE and the Global Commission on the Stability of Cyberspace (GCSC) can be viewed as responding to these calls, as can UNIDIR's annual cyber stability conferences. As with the section on private sector, Table 1 in the Annex identifies those norms around which participants at the first meeting of the Geneva Dialogue believe these different actors already contribute through their own work, or where greater interaction can be fostered in support of their implementation.

- The Geneva Dialogue might consider further discussion of the sources of legitimacy and authority of civil society (in the broad understanding of the term) in driving responsible behaviour in cyberspace. For example, when it comes to the implementation of the UN GGE recommendations on international law, norms and CBMs, is the contribution of civil society substantial or incidental, merely a matter of creating the right 'atmospherics'? What is the risk that these actors can be co-opted by government actors, political parties, foreign actors or the private sector (through funding, campaigns, etc.)?

Other Outstanding Issues:

- The Geneva Dialogue workshop demonstrated that there is a lot of interest amongst civil society actors in exercising oversight of government actions and pushing for greater accountability and transparency (e.g. in the area of surveillance) or engaging in/ influencing processes such as the UN GGE and the Open Ended Working Group (OEWG). However, participants at the workshop agreed that civil society currently has no coherent strategy for either conducting effective oversight or for engaging with the First Committee processes, including around specific thematic issues (e.g., human rights, critical infrastructure protection, crisis management, confidence building or other). Furthermore, efforts of civil society organizations are sometimes duplicated due to lack of capacity or a lack of coordination.

- A key focus for the Geneva Dialogue in future could be to deepen understanding of what works/ does not work in the area of civilian oversight and what the objective of greater coordination amongst civil society would be (e.g., issue-specific such as human rights, confidence building or crisis management?). Should an attempt be made to organise the different contributions made by civil society into something more homogeneous and coherent, or does the strength of the civil society contribution lie in its diversity?

- There appears to be a lot of coherence (and trust) within the technical community. Several participants from the technical community noted how there is limited awareness among the technical community of the UN First Committee processes and how their work contributes to implementing the recommendations of the UNGGEs and broader international security and stability. A future focus of the Geneva Dialogue could be to identify good practices of trust building and cooperation within the technical community and their relevance to the work of the UN GGE and the Open-Ended Working Group.

[38] UN GGE 2015, paras 23 and 31.

- Participants at the Geneva Dialogue workshop noted how (some) government agencies are increasingly willing to engage with civil society to pursue common goals. However, meaningful collaboration is often lacking, sometimes because civil society delegates perceive that they are not treated as equals or that direct communication lines between civil society and governments are sometimes insufficient. Future discussions within the framework of the Geneva Dialogue could focus on how cooperation with or partnerships among civil society actors and between governmental agencies or private sector can be rendered more transparent and more effective.

SECTION 4: OVERARCHING ANALYSIS AND NEXT STEPS

The best approach to responsible behaviour in cyberspace is contained within the idea of a 'framework' or, more usefully, a 'regime'. A regime-based approach not only spans the range of obligations from the 'hard' (i.e. legally binding) to the 'soft' (i.e. politically binding or voluntary norms), it is also politically pragmatic in that it allows for priorities to be set within a widely understood framework of acceptable behaviours and allows for those priorities to change as circumstances demand. Furthermore, the regime can tolerate a level of difference and disagreement, and even tension. And given that the regime is based on some level of consensus, it also has the in-built capacity for dispute resolution. Steven Krasner defined 'regime' in the following way:

> Implicit or explicit principles, norms, rules and decision-making procedures around which actors' expectations converge in a given area of international relations. Principles are beliefs of fact, causation and rectitude. Norms are standards of behaviour defined in terms of rights and obligations. Rules are specific prescriptions or proscriptions for action, decision-making procedures are prevailing practices for making and implementing collective choice.[39]

Complex as they are, the responsibilities highlighted above (international law, norms, CBMs etc.) already form the basis for an emerging framework or 'regime' of responsibility in cyberspace and for contributing to greater peace, security and stability. Some refer to this framework as a 'stability framework'.

States have the legitimacy and capacity to create a 'responsibility regime' at the domestic level. Furthermore, implementing the emerging framework or regime of 'responsibility' offers the most hopeful path to international collaboration in pursuit of peace, security and stability in cyberspace. Allowance must be made for governments to prioritise among the broad range of requirements and expectations, other than in the case of unequivocally binding legal obligations. It follows that at the international level (other than in the case of uncontested, unequivocal legal obligations) allowance must be made for states to adopt contingent approaches to responsibility.

Regardless of this emerging framework, irresponsible behaviour on the part of States persists and remains potentially destabilizing.

- What incentives exist for promoting more responsible behaviour?
- What are the costs (e.g. national level deterrence frameworks) associated with irresponsible behaviour?

Striking a Balance

States have discrete/unique responsibilities regarding ICT, particularly when it comes to national and international security. These responsibilities, many of which derive from the UN Charter and other existing international law must be acknowledged and implemented. The emerging normative framework developed through the work of the UN GGEs is important, as is the normative and cooperative work underway at regional level (ARF, OAS, OSCE, SCO), although it is imperative to move from ambition to implementation. It will also be important to ensure coherence between existing mechanisms and the work that will be undertaken by the new mechanisms (OEWG and GGE) approved by the UN General Assembly's First Committee. States cannot expect to be responsible for everything, not least because the underlying architecture and technology products and services are developed by and owned by private actors, who themselves have (or should have) obligations and responsibilities toward the users of the underlying ICT architecture, and associated products and services. These responsibilities will (or should) grow in tandem with society's technological dependence.

[39] S. Krasner, 'Overviews', in S. Krasner (ed.), *International Regimes* (London: Cornell University Press, 1983), p.2.

Given the character of the ICT environment, it is imperative to strike a balance between responsibilities (the balanced 'responsibility regime'). This will require states engaging other actors, as per the recommendations of the GGE reports. For instance, a balanced 'responsibility regime' requires closer engagement of technology companies – through norms, regulation/other enablers of responsibility. It also requires closer engagement of other actors who not only ensure the smooth functioning of the internet but who are also first responders in the event of incidents. And those who can identify looming threats and normative dilemmas and push for accountability and transparency of state and corporate action. The table in Annex 1 outlines just some of the ways private sector and civil society actors engage with the norms recommended in the 2015 GGE report, even if the latter was directed at states. The work of multi-stakeholder groups such as the GCCS or the French 'Call' serve important purposes in bringing forward existing norms and proposing new ones.

Closing the Responsibility Gap(s)

Despite important steps taken by groups of states to protect citizens and enhance privacy (EU NIS Directive, GDPR), the gap between normative aspirations and actual state practice is, however, growing. It is difficult to understand what progress is being made to implement the package of norms recommended in the 2015 GGE report since very few states have articulated what they are actually doing in this regard. While this is somewhat to be expected with regard to the limiting norms (i.e. the norms of restraint), discussing or articulating implementation of the positive duties that form part of the package should be more straightforward.

Many states across the globe have not met their responsibilities vis-a-vis citizens, who continue to be the most constant targets of malicious ICT activity by States.

Several States continue to engage in offensive or disruptive action – each time with higher financial and political costs - which in turn has raised questions about the usefulness of the norms (some would argue that based on the effects of these incidents, significant restraint is being demonstrated). In response, there is an emerging trend amongst some states to adopt policies of consequences, i.e., responding to irresponsible behaviour and disregard for norms of restraint through public attribution followed by punishment (sanctions and offensive action). Evolving concepts such as persistent engagement are also understood in this light. Deterrence is an option but has been criticised as there are too many uncertainties attached. As noted, there is growing concern that these and other developments are resulting in a complex security dilemma. The current situation highlights a high potential for constant friction; and by extension, a high potential for escalation, especially if the activity is affecting critical energy, finance or military-dependent C2 systems. It is unclear that our political institutions are prepared to manage constant friction and crisis.

As a means to contribute to closing the responsibility gap, the Geneva Dialogue could focus on the following questions. Doing so could well serve as a much-needed stimulus to current discussions on norm implementation, and could put some parameters around otherwise complex obstacles:

- Do the three constituencies (States, Private Sector, Civil Society) demonstrate a shared or broadly similar understanding of 'an open, secure, stable, accessible and peaceful cyberspace', particularly when it comes to international peace and security?
- Given the extent of our reliance on ICT, can an offensive posture – including for activity below the IHL/LOAC threshold – be realistically and credibly combined with one that promotes norms of restraint?
- In the current environment, is it possible to model alternative incentive structures to shift current behaviours towards the kinds of engagements we need for greater stability and security in cyberspace?
- What can be done to strengthen confidence building, crisis management and related dialogues and processes (diplomatic, military, cross-agenda) for dealing with the growing possibility of

escalation? What role can private sector and civil society actors play in these dialogues and processes?
- Do current mechanisms (domestic and international) engage adequately with the full range of challenges, e.g. state-sponsored subversion?
- Are there areas in which states, the private sector and civil society actors should not seek to be involved, i.e., are there roles and responsibilities which each of these constituencies should perhaps leave to others?

Systemic challenges relating to the underlying technological substrate continue to be the main drivers of instability and insecurity, and tip the balance in favour of offense over defence. Current initiatives (normative, technological/security) by different actors are insufficient and questions abound regarding their sources legitimacy around what they are actually achieving. This situation will grow more complex alongside growing dependency on technology and greater advances in technology.

- How to balance this reality with a balanced responsibility regime? Are state authorities fully open to collaboration with the private sector in ensuring greater security and stability in cyberspace? How might greater collaboration between the public and private sectors be applied to meeting the challenge of attribution?
- How can the disjunction between micro-level and macro-level efforts to deal with technological vulnerabilities be approached? The Geneva Dialogue might assess ongoing efforts such as national-level Vulnerability Equity Processes and Coordinated Vulnerability Disclosure initiatives, and identify other approaches involving the technology sector that address vulnerability challenges and associated risks.
- Obligation versus expectation: is 'responsibility' something to be regulated and enforced, or preferred and encouraged? For example, should more "proactive responsibility" and accountability levers be introduced via the ICT marketplace or should they be left to national (regulation, taxation, certification), regional and international levers (EU, WTO)?[40]
- How can the Geneva Dialogue contribute to deepening understanding of what works/ does not work in the area of civilian oversight?

The UN GGE reports were explicit on the role of other actors in supporting implementation of some of the recommendations listed in the reports. The norms of responsible behaviour recommended in the 2015 report are directed at states but some imply the involvement of other actors. Yet awareness of the norms is still limited. Beyond the private sector, specific references are made in the reports to civil society, academia, research institutes and think-tanks, and technical actors such as CERTs and CSIRTs. The reports suggest studying the possibility of establishing mechanisms to facilitate such engagement or participation. To date, no mechanism has been established, although that is not to say that some countries have not established their own mechanisms to consult with or engage these different actors at national level. Both the OEWG and GGE set to commence work in 2019 have contemplated consultation mechanisms. The OEWG in particular discusses the need to consult with key actors such as the private sector as well as civil society. Work is probably underway to determine the modalities to use in this regard, although the 'what, why and how' of such consultations will be imperative moving forward.

- How do the UN and UN member states envisage this kind of engagement?
- How do these actors themselves envisage interacting with the two mechanisms? What are the sources of legitimacy and authority of private sector actors and civil society (in the broad understanding of the term) in driving the UN debate on responsible behaviour? For example, when it comes to the implementation of UN GGE recommendations on international law, norms and CBMs, is the

[40] The authors are grateful to John Mallery for his insightful contributions on this topic made at UNIDIR Cyber Stability Conference 2018: Preventing and Mitigating Cyber Conflict.

contribution of civil society substantial or incidental, merely a matter of creating the right 'atmospherics'? Should governments that most publicly advocate the multistakeholder approach to the governance and security of cyberspace be expected to ensure that their delegations to GGE and OEWG deliberations have a suitably broad base of participation, including representatives from civil society, academia and the technology communities?

- How can platforms such as the Geneva Dialogue promote greater awareness of the norms of responsible behaviour recommended by the UN GGEs, and facilitate dialogue between different actors and identify good practices in their operationalisation/implementation? How can the Geneva Dialogue engage actors from other key sectors – energy and finance –also viewed as critical to international stability and security – in the Geneva Dialogue? What about the insurance sector?
- A number of complementary self-regulatory initiatives such as the recent Paris Call for Trust and Security in Cyberspace, the Siemens Charter of Trust, the Cybersecurity Tech Accord, the Digital Peace Now campaign and Kaspersky's Transparency initiative have been promoted by or involve the technology sector. Understanding their impact and their contribution to international security and stability is crucial yet, at present, there is limited reporting on what they have achieved. How might platforms such as the Geneva Dialogue contribute to ensuring greater transparency around these initiatives?

The growing digitalisation of our societies and economies – and our conflicts - creates a slew of new challenges: new threats and vulnerabilities are emerging around IoT, where the line between human agency and 'smart agent-like devices' is becoming increasingly blurred and the safety and security of related services and devices remains a serious problem. Novel threats are also emerging around AI-dependent critical systems (e.g. the growing cloud-based industry); critical satellite systems; and information and decision-making processes, which are increasingly manipulated for political and strategic effect".[41]

- Do current mechanisms (domestic and international) engage adequately with the full range of challenges?
- And in what ways will the current debate on state responsibility be affected by emerging challenges posed by the Internet of Things and by AI-enabled infrastructures, quantum computing and encryption?

Next Steps for the Geneva Dialogue

The first Geneva Dialogue workshop was well-attended by representatives of the different stakeholder communities.[42] A key observation from the 1.5 days is that there is significant interest in the topic of the workshop, i.e. the roles and responsibilities of the different stakeholders in cyberspace and how these responsibilities interact (or don't). The Concept Note developed for the conference served as a very solid basis for discussions. Undoubtedly, the topic of the workshop is complex, and discussing it with different stakeholders who do not necessarily represent the multiple actors and interests within a given stakeholder group is challenging.

During the workshop, discussions centred principally on i) how to contribute to operationalising the norms of responsible state behaviour recommended by the 2015 GGE and determine modes of interaction/cooperation with the roles and responsibilities of other key actors/sectors; and ii) whether/how to take the Geneva Dialogue initiative forward in a manner that is outcome oriented.

[41] C. Kavanagh, 'New Tech, New Threats: Insights for the UN Secretary-General and his High-Level Panel on Digital Cooperation' (forthcoming).

[42] States represented included France, Germany, Israel, Kenya, the Netherlands, Mexico and the United Kingdom. The United States, Russia and China were invited to send representatives. Companies represented include Huawei, Kaspersky, Kudelski, Microsoft, Swift, Swissgrid and Telefonica. The technical community was also represented, including by APNIC, FIRST, HEIG-VD, the Institute for Security and Safety and Namibia University of Science and Technology. Civil society was represented by organisations such as Citizen Lab, Global Partners, ICRC, ICT4Peace, the Just Net Coalition and the World Economic Forum. Academia and policy research think-tanks included CCDCOE, CEIP, EUISS, the Hoover Institute and the Universities of Cambridge and Lausanne.

There was broad consensus that the Geneva Dialogue should focus on responding to the questions outlined above; distilling and sharing good practices of responsible behaviours (for instance, on policy, legislation, cooperative mechanisms etc.) that contribute to implementing specific norms; and identifying practices of cooperation and collaboration with other actors in the process. Such an approach would be possibly more conducive to drawing in other actors. Determining how to better engage different types of actors within the three stakeholder groups would be important, as will keeping the initiative tied to international security and managing expectations.

Finally, the workshop discussed the feasibility of using the initiative as an input to the UN Open-Ended Working Group (OEWG), the GGE, and the envisaged consultation mechanisms. There was interest in such an approach, if the Geneva Dialogue determines how to best complement other initiatives such as the Paris Call, the GFCE, the GCCS and the London Process.

ANNEX 1: UN Group of Governmental Experts Norms (2015)[43] – Private Sector and Other Participation. PROVISIONAL FINDINGS

Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. Part III, Paragraph 13: Norms, Rules and Principles for the Responsible Behaviour of States

13 (a)	Consistent with the purposes of the United Nations, including to maintain international peace and security, States should cooperate in developing and applying measures to increase stability and security in the use of ICTs and to prevent ICT practices that are acknowledged to be harmful or that may pose threats to international peace and security			
	PRIVATE (TECH) SECTOR		**OTHER ACTORS**	
	Extant/Assumed R&R	Prospective R&R	Extant/Assumed R&R	Prospective R&R
			- Research	- Establish mechanisms to engage with GGE/ other - Monitor state implementation of the norms, including mechanisms of international cooperation
13 (b)	In case of ICT incidents, States should consider all relevant information, including the larger context of the event, the challenges of attribution in the ICT environment and the nature and extent of the consequences.			
	PRIVATE (TECH) SECTOR		**OTHER ACTORS**	
	Extant/Assumed R&R	Prospective R&R	Extant/Assumed R&R	Prospective R&R
			- Research	- Contribute with the private sector to establish frameworks for attribution including common standards for reaching an attribution finding; (technical, legal and political considerations).
13 (d)	States should consider how best to cooperate to exchange information, assist each other, and prosecute terrorist and criminal use of ICTs and implement other cooperative measures to address such threats.			
	PRIVATE SECTOR		**OTHER ACTORS**	
	Current R&R	Prospective R&R	Extant/Assumed R&R	Prospective R&R
	- Forensics - PPPs with law enforcement, IRUs etc. - Self-regulation (GIF, ToS etc.) - National regulation/ legislation		- Research, inc. on IL (e.g., work of the ILC) - Security research - Technical support to victims - Incident response (CERTs)	

[43] UN General Assembly, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (UNGA: A/70/174, 22 July 2015), pp.7-8. Available at: http://undocs.org/A/70/174

13 (g)	States should take appropriate measures to protect their critical infrastructure from ICT threats, taking into account General Assembly resolution 58/199 on the creation of a global culture of cybersecurity and the protection of critical information infrastructures, and other relevant resolutions.			
	PRIVATE SECTOR		**OTHER ACTORS**	
	Current R&R	Prospective R&R	Extant/Assumed R&R	Prospective R&R
	- Maintain and ensure resilience of critical infrastructures - Warn of and patch known hard-/software vulnerabilities	- Develop products with due regard for security and maintain legacy systems - Support attribution efforts - Refrain from security-endangering offensive measures and subversive actions (e.g. hack-backs) - Provide active assistance in implementing norms of responsible behaviour - Refrain from backing state actors in offensive activities - Contribute to ensuring supply chain integrity		- Academia and civil society could help develop practical tools and guidance, and describe basic measures to share information on cyber risks, malware, etc.
13 (h)	States should respond to appropriate requests for assistance by another State whose critical infrastructure is subject to malicious ICT acts. States should also respond to appropriate requests to mitigate malicious ICT activity aimed at the critical infrastructure of another State emanating from their territory, taking into account due regard for sovereignty.			
	PRIVATE SECTOR		**OTHER ACTORS**	
	Extant/Assumed R&R	Prospective R&R	Extant/Assumed R&R	Prospective R&R
13 (i)	States should take reasonable steps to ensure the integrity of the supply chain so that end users can have confidence in the security of ICT products. States should seek to prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions			
	PRIVATE SECTOR		**OTHER ACTORS**	
	Extant/Assumed R&R	Prospective R&R	Extant/Assumed R&R	Prospective R&R
	- Tech Accord	- Refrain from security-endangering offensive measures and subversive actions (e.g. hack-backs) - Refrain from backing state actors in offensive activities - Contribute to ensuring supply chain integrity		
13 (j)	States should encourage responsible reporting of ICT vulnerabilities and share associated information on available remedies to such vulnerabilities to limit and possibly eliminate potential threats to ICTs and ICT-dependent infrastructure			
	PRIVATE SECTOR		**OTHER ACTORS**	

	Extant/Assumed R&R	Prospective R&R	Extant/Assumed R&R	Prospective R&R
	- Tech Accord - MSFT Digital Peace Campaign			- Develop frameworks to report and remedy ICT vulnerabilities.] - Conduct research/ motivate discussion on what constitutes responsible reporting and how might it be monitored by civil society and on the rules of engagement that should apply between private and public sector actors ~~to illuminate~~ with for disclosing and remedying vulnerabilities?
13 (k)	States should not conduct or knowingly support activity to harm the information systems of the authorized emergency response teams (sometimes known as computer emergency response teams or cybersecurity incident response teams) of another State. A State should not use authorized emergency response teams to engage in malicious international activity.			
	PRIVATE SECTOR		**OTHER ACTORS**	
	Extant/Assumed R&R	Prospective R&R	Extant/Assumed R&R	Prospective R&R
				- The technical community could develop a form of "rapid reaction plan" for those cases is which CERTs are used to conduct attacks on others (CERTs or otherwise)? If that norm is violated, the technical community could rapidly react and document the activities. - Report on ICT-related vulnerabilities and back these documents with evidence-based research.