Geneva Dialogue on Responsible Behaviour in Cyberspace: Civil Society

Framework Document, November 2018

Author:

Prof. Dr. Solange Ghernaouti

Swiss Cybersecurity Advisory and Research Group (www.scarg.org)

Fondation SGH – Institut de recherche Cybermonde (fondationsgh.org)

UNIL | Université de Lausanne

Table of Content

1 Introduction and Purpose

The Swiss Federal Department of Foreign Affairs has launched the Geneva Dialogue on Responsible Behavior in Cyberspace in order to explore the roles and responsibilities of three stakeholder levels: states, private entities and civil society.

In light of the workshop planned for 1 and 2 November 2018, the University of Lausanne has been enlisted to lead Workstream 3, which will illuminate the roles and responsibilities of civil society in the context of international peace and security.

The interdisciplinary nature of cyberspace requires the engagement of a diverse range of stakeholders from both public and private spheres. In recent years, involvement of academics, social scientists, private firms and other non-state actors in the international cyber security debate has increased considerably. And yet, the University of Lausanne's analysis indicates an untapped potential for civil organizations to expand their engagement, especially in the international debate on norms of conduct, confidence-building between states and capacity building[1].

While discussions on responsible behavior have gained international traction, the international diplomatic cyber stability agenda's focus has thus far been on clarifying appropriate state-level conduct regarding information and communication technologies (ICTs) and their many uses. The attendant UN process has been instrumental in developing cooperative measures such as norms of responsible state behavior. The UN GGE report issued in 2015 affirmed 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 of the private sector, academia and civil society organizations."

Therefore, the Geneva Dialogue on Responsible Behavior informs the international community by going beyond the traditional state-centric focus and outlining other actors' impacts on international peace and security. Broadening both the themes under discussion and the stakeholder base is a timely development: private entities and representatives of civil society have long called for more transparent and inclusive processes pertaining to the international and regional cyber security agenda. As technological advances (e.g., the Internet of Things and Artificial Intelligence) have surpassed the capacities not only of regional/international organizations but of states to unilaterally formulate efficient, swift and appropriate responses, the inclusion of civil society would be mutually beneficial: diplomatic processes would gain in legitimacy, accountability and transparency, while the societies they serve would benefit greatly from increased stability and security.

This paper discusses civil organizations' roles, responsibilities and possible contributions regarding international cyber stability. For the purposes of this document, the roles of civil actors will be limited to tasks and objectives conducive to international cyber stability. The goal of this entire process is to allow all stakeholders – state and non-state, large and small – access to cyberspace's burgeoning opportunities. This will mean developing systems wherein the incentives to cooperate and collaborate outweigh those to engage in malicious or predatory activities[2].

---

[1] Schjolberg S., Ghernaouti-Hélie S. (2009). A Global Treaty on Cybersecurity and Cybercrime. A contribution for peace, justice and security in cyberspace. Cybercrimedata https://www.researchgate.net/publication/236200268_A_global_treaty_on_cybersecurity_and_cybercrime

[2] United States, Department of State, International Security Advisory Board (2014). Report on A Framework for International Cyber Stability. Retrieved from https://www.state.gov/documents/organization/229235.pdf

2 Context

Information and communication technologies (ICTs) have become so integral to modern society that it is difficult to imagine life without them. Digital devices play decisive roles in how people communicate and establish social contacts, as well as in how political messages are expressed. Demanding a very small investment in infrastructure, cyberspace allows its users to share information, interact, swap ideas, play games, engage in social forums, conduct business and voice political opinions. No previous medium has given common people such power either to access information or to disseminate it. Moreover, digitization not only promotes economic growth, but drives innovation and knowledge – including concepts of human rights. For these to be realized, though, one essential precondition is a dynamic balance between access to information, individual privacy, free expression, economic wellbeing and security at every level[3].

For all of its advantages, of course, cyberspace is a double-edge sword. Like most technological advancements, digitization has been accompanied by negative side effects. As individuals, public entities and private organizations and national structures have benefitted from ICTs, they must also manage the associated risks.

Recent examples, such as the WannaCry and NotPetya ransomware attacks, have illustrated how vulnerable societies are: critical infrastructures can be compromised, preventing delivery of essential services such as healthcare and energy. Global digital connectivity, vulnerabilities of digital devices, the high degree of anonymity and the possibility of deniability, make it possible for malicious actors to exploit ICTs' vulnerabilities for strategic ends. Not only large-scale malicious cyber activities, but the need to be vigilant against them have negatively impacted international peace and stability. This is not only because they have become a daily occurrence, affecting individuals and societies alike, but because they have eroded people's faith and confidence in democratic political institutions' capacities to protect them.

ICT weaponry has been a feature of international conflict for at least two decades: as early as 1998, they have been integrated into military operations during conventional armed conflicts. Examples include the Kosovo war in 1998, the outbreak of the Second Intifada (1999) and Russia's conflicts with Georgia (2018) and Ukraine (since 2014).

More commonly, though, countless incidents, operations and activities conducted below the threshold of armed conflict make war- and peacetime very fluid concepts, while making it extremely difficult for states to employ the full gamut of military and cyber-countermeasures. Known examples include targeted operations against critical infrastructures in Estonia (2007) and Iran (2010).

As noted above, the growing popularity of malicious cyber activities and operations as means of achieving strategic ends and furthering political, military and economic interests has diminished people's confidence in their governments' abilities to protect them. Further decreasing citizens' trust in democratic institutions and outcomes, the Snowden leaks revealed blanket surveillance practices even in developed democracies.

Most importantly, civil groups are often direct targets of malicious activities conducted by state-supported actors. The University of Toronto's Citizen Lab[4] has been particularly vocal about threats directed against non-government, non-military targets. According to this research-based institute, civil society is particularly vulnerable to such targeted operations because they often lack the capacity or knowledge to identify and counter them.

Against this backdrop, various members of the international community have collaborated on a diplomatic agenda to trace the bounds of acceptable behavior regarding ICT use. As states have the

[3] Ghernaouti, S. (2013). Cyberpower, Crime, Conflict and Security in Cybersapce. EPFL Press.
[4] https://citizenlab.ca/

"primary responsibility for the maintenance of international peace and security, including the maintenance of "a secure and peaceful Information and Communication (ICT) environment"[5], they have been the primary subject of this normative debate.

In cyberspace, however, the state is only one class of actor among many: the Internet is an environment owned by many stakeholders, similar to a condominium complex.[6] Most of the routers, physical hardware and access-related expertise are in the hands of private sector firms, often large telecommunication and internet service providers, and academic institutions. Their users – most of whom are non-state actors – depend on these systems continuously, making them a subject of national and international security discourse.

Clearly, the governmental purview lies in ensuring security, upholding the rule of law and respecting and protecting human rights. And yet, the cyberspace's polymorphic nature makes it impossible for any government to adequately address all risks, behaviors, processes or outcomes as they develop. However, civil society groups tend to be better-positioned to do these jobs, as they often enjoy higher credibility, and have more experience engaging directly with specialized groups (e.g., technical communities) and addressing the challenges posed by ICT misuse.

3 Definition of Civil Society

The term "civil society" has recently seen a surge of use in discussions of democratic processes around the globe[7]. However, the concept it signifies is rather nebulous. Of the numerous ways of conceptualizing and defining it, the majority spring from three sources. The first, provided by Marx, focuses on a non-state sphere of influence that originates in capitalism and industrialization. The second is a normative approach, the dominant purpose of which is to judge states' behavior in relation to their citizens. This definition deals with states' capacities to ensure that their constituent individuals' and groups' rights are not abused. The third is provided by social science. According to this definition, civil society mirrors the "interaction of voluntary groups in the non-state sphere" [8]. The sociologist Thomas Janoski[9] conceptualizes it as a sphere of "dynamic and responsible public discourse between the state, the public sphere consisting of voluntary organizations, and the market sphere concerning private firms and unions" (p. 12). As it is difficult to define precisely what civil society is, it is often characterized in terms of what it is not, e.g., "non-military", "non-violent", or "non-profit".

For the purpose of this framework document, civil society is a sphere of social life involving voluntary non-state organizations[10] that can act both in relation to the state and as legal entities in relation to the economy. The societal sphere further encompasses private associations: it is a space for individuals to aggregate shared interests and goals so that they can advance in a coordinated way[11]. Civil society is motivated to shape policies and processes without competing with states and governmental tasks.

---

[5] UN GA, A/70/174 (2015). Group of Governmental Experts on Developments in the Field of Information and Telecommunication in the Context of International Security. http://undocs.org/A/70/174

[6] Lewis, J.A. (2010). Cybersecurity: Next Steps to Protect Critical Infrastructure. https://fas.org/irp/congress/2010_hr/cybersec.pdf

[7] See for example Meltz, D. (2016). Civil Society in the Arab Spring: Tunisia, Egypt, and Lybia. https://scholar.colorado.edu/cgi/viewcontent.cgi?article=2301&context=honr_theses

[8] In Janoski, T. (1998). *Citizens and Civil Society: A Framework of Rithgs & Obligations in Liberal, Traditional and Social Democratic Regimes*. Cambridge University Press.

[9] Ibid

[10] Political groups, religious organizations, educational institutions, community service associations, grassroots organizations, etc.

[11] See Concept Paper for Geneva Dialogue on Responsible Behavior in Cyberspace (p.1).

4 Role of Civil Society

The role of civil society that pertains most directly to international security has varied across time and regions. During the 20th century, civil society groups and organizations were mostly associated with industrialized Western democratic states. During interstate wars, for instance, one of the tasks performed by these organizations was to support war efforts[12]. Another role of civil society has long been to mobilize with the aim of bringing about an end to war or an unjust political order. One example from the pre-digital period is the Polish trade union's commitment to peaceful change during the Solidarity Movement of 1989-1990[13]. At the time, it was considered miraculous that, with virtually no positive coverage via (state-controlled) mass media, such a movement could succeed. In recent years, though, with large numbers of people able to afford access to digital ICTs it has become far more common for intrastate conflicts to involve factions of civil society who use social media to catalyze political transitions[14] especially from totalitarian[15] to democratic systems. Thus, civil society has played an important role in a whole-of-society approach to preventing conflicts and mitigating nascent crises.

In the cyber security realm, the importance of participatory civil society has been acknowledged by governments, as articulated in international and regional multilateral processes. This is an important message: while governments consider that civil society has traditionally only occupied physical space, more often than not, they acknowledge that the Internet and the ICTs that underpin it have nevertheless impacted people's societal engagement and altered the way they advance their goals. In 2017, worldwide Internet users numbered around 3.4 billion, many of them active in social media[16].

One of the most salient outgrowths of Internet use is the growth and spread of social media communities, i.e., groupings that transcend geographical distance and social divides. As these communities encourage their members to connect formally and informally, and to expand their networks of connections, they make it very easy to mobilize support and commitment.

Therefore, it should come as no surprise that civil society's engagement in the international diplomatic agenda regarding peace and security in cyberspace can be improved. Adding to the value they bring to discussions on international peace and cybersecurity, civil society groups commonly share extensive expert knowledge and experience developing programs that promote peace. Usually locally rooted and well-versed in local dynamics and trends, they have the legitimacy and influence to address national concerns at a "grass roots" level. Thus, they can serve as early warning mechanisms for emerging threats[17]. While their immediate priorities are typically local, their connectedness facilitates work across nations, communities and disciplines.

The following areas delineate some of the roles played by civil society groups[18]:

---

[12] The support of American Enterprise Institute, a foreign policy think tank, of US invasion of Afghanistan in 2001 and Iraq 2003. http://www.aei.org/about/

[13] See for example: Bartkowski, M. (2009). Poland's Solidarity Movement (1989-1990). International Centre on Nonviolent Conflict. https://www.nonviolent-conflict.org/wp-content/uploads/2016/02/Poland-Solidarity-Movement.pdf

[14] Example is: Women's Coalition which led the Yes! Campaign in Northern Ireland which contributed to the 1998 Good Friday Agreement, a major political development in the Northern Ireland peace process.

[15] See Meltz, D. (2016). Civil Society in the Arab Spring: Tunisia, Egypt, and Lybia. https://scholar.colorado.edu/cgi/viewcontent.cgi?article=2301&context=honr_theses

[16] https://www.statista.com/statistics/273018/number-of-internet-users-worldwide/

[17] OSCE (2018). The Role of Civil Society in Preventing and Countering Violent Extremism and Radicalization that Lead to Terrorism: A Focus on South-Eastern Europe. https://www.osce.org/secretariat/400241

[18] The upcoming paragraphs are drawn from the following paper: Kavanagh, C., Stauffacher, D. (2014). A Role for Civil society? ICTs, Norms and CBMs in the context of international security.

4.1 Effective Engagement and Participation

Civil society groups can lobby for seats at the table of existing multilateral processes, either as observers or as active participants.

Their members can participate in government delegations during negotiations of cooperative measures such as norms, capacity building measures (CBMs) and capacity building programs.

They can also support governments ahead of negotiations via expert round tables.

They can organize and demand hearings before and after government participation in CBMs, norms of responsible state behavior and other cyber security-related processes.

They can be organized and coordinated in permanent multilateral institutional structures (for example, advisory boards, sub-working groups to foster implementation of specific cooperative measures/CBMs).

They can act as spokespeople for other interest groups, such as computer emergency readiness teams (CERTs), and liaise between the technical community and policy makers.

4.2 Awareness Raising and Capacity-Building

Civil groups can focus their messages by partnering with think tanks and specialized organizations such as the Geneva Centre for Security Policy and the ICT4Peace Foundation. These organizations will allow them to help tackle states' incapacities to keep pace with the international diplomatic agenda on cyber security. For example: Programmes such as the International Cyber Security Capacity Building Workshops. Organized by the ICT4Peace Foundation with joint governmental support, these are offered to enhance the understanding of practitioners, diplomats and other representatives of civil society regarding ongoing international processes that promote confidence building measures, norms of responsible state behavior and international cooperation in cyberspace.[19] .

They can gain access to developments and activities through observatories. For example, the Geneva Internet Platform[20] (GIP) Digital Watch observatory 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.

As well as academia, research institutions and foundations[21], they can assist their states in their efforts to improve ICT security regarding cybersecurity and strategies, development of a cyber culture and society, legal frameworks, standards, organizations and technologies.

---

[19] The ICT4Peace capacity building program envisages broadening participation in international cyber security debates, negotiations at regional and global levels, and multilateral forums such as the OSCE and the UN GGE. The workshops, which can be organized with the support of regional organizations including the OSCE, the OAS and the AU, are also intended to increase the understanding of ICT-based security threats and regional concerns, while sharing best practices and institutional arrangements to cope with the related risksICT4Peace (2014). International Cyber Security Capacity Building Workshops.
Promoting Openness, Prosperity, Trust and Security in Cyberspace.http://ict4peace.org/wp-content/uploads/2017/10/Outline-Capacity-Building-2017811.pdf

[20] https://www.giplatform.org/

[21] Ghernaouti, S., Wanner B. (2018) « Research and educaton as key success factors for developping a cybersecurity culture » in Cybersecurity best practices, p.539-551 Springer Vieweg.

They can organize events in support of ongoing negotiations. For example, CBM 1 of the OSCE set encourages states to share information on perceptions regarding national threats. Drawing on the expertise of private entities, CERTs, etc., civil society groups could help collect relevant information about existing and potential threats.

4.3 Diplomacy

Particularly in situations where the political climate does not allow for direct state-to-state exchanges, civil society can facilitate interstate dialogue. Track 1.5 and 2 dialogues can help create an environment where states can confidently address issues in a frank and open manner. The Sino-European Cyber-Dialogue is a good example of how civil society groups can serve a diplomatic purpose.

These and similar groups can promote policy outcomes that would otherwise be difficult due to current international relations, while promoting adherence to and implementation of policy outcomes.

Civil society can further help bring about policy outcomes that would otherwise be difficult due to current international relations. As related groups can promote adherence to and implementation of policy outcomes[22], they can also facilitate Track 1 dialogue through mediation.

4.4 Accountability and Monitoring

Civil society groups can monitor and report on states' and private sector actors' implementation of norms and standards to which they have committed.

By monitoring and reporting on states' and private sector actors' implementation of norms and standards to which they have committed, civil society groups' can help measure programmatic effectiveness for impact assessments. Cyberspace's general fluidity normally makes that task very challenging.

4.5 Transparency

Regional organizations (e.g., the OSCE) have often served as platforms to share information on states' respective threat assessments (CBM 1), as well as on policies, capacities, strategies, etc. (CBM 7). One purpose of this choice is to promote states' openness about their intentions, thereby increasing predictability. Moreover, Points of Contact (CBM 8) have already been nominated at the technical and policy levels. Against this background, as a step toward formulating best practices, raising aware-ness or even designing capacity building activities, civil society actors could compare information shared on the implementation of cooperative measures.

Perhaps most importantly, such non-government actors can monitor and publicize state-level practices that negatively impact civil society itself. The Citizen Lab, for example, helps investigate state-sponsored malicious cyber activities that impact online freedom of expression. Through similar activities, particularly regarding state-corporate positions on online privacy and information control, civil organizations can increase transparency and accountability.

5 Challenges (Principle Based Engagement)

5.1 Lack of Legitimacy and Credibility of Civil Society Actors

- This can result from lack of clarity of institutional goals and mandates.

[22] Example: The International Campaign to Abolish Nuclear Weapons (ICAN) is a coalition of non-governmental organizations has been instrumental in promoting adherence to and implementation of the United Nations nuclear weapon ban treaty.

5.2 Lack of inclusion

- A whole-of-society approach can be improved on when developing national and international policies pertaining to international peace and cybersecurity.
- Timely inclusion is lacking at the strategic and policy levels (improvements have been included in the policy drafting process).

5.3 Interplay between Civil Society and Governmental Agencies

- The relationship between government and civil society has improved.
- Government agencies are often willing to engage with civil society to pursue common goals.
- Meaningful collaborations are lacking, sometimes because civil society delegates perceive that they are not treated as equals.
- Direct communication lines between civil society and governments are sometimes insufficient.

5.4 Duplication of work

- Efforts of civil society organizations are sometimes duplicated due to lack of coordination.

5.5 Sustainable Funding

- Long-term participation and engagement of civil society requires reliable funding and long-term commitment, ideally originating from various sources (to maintain independence).

5.6 Neutrality

- Partnerships among civil society actors and between governmental agencies or private sector should be fully transparent.
- Such partnerships should be based on trust and a climate of non-instrumentalization.
- Relations should be based on cooperation/coordination rather than on instructions and directions.

6 Observations and Preliminary Suggestions to Improve Civil Society's Roles in Cyber

6.1 Conducive Environment

- Civil society-led programs and tasks need to be performed in an environment in which actors do not fear interference and where fundamental rights, such as privacy, freedom of expression, assembly and association are respected and protected.

6.2 Facilitation of Civil Society's Involvement

- Governmental entities should focus on creating the conditions necessary to involve civil society across the full spectrum of policy development.
- Partnerships and platforms for collaboration could be established/improved. Governments can facilitate trust-building with civil society and better integrate their involvement in implementation efforts regarding normative instruments

- Coordinated multi-agency mechanisms should be established. Examples include periodic roundtables and platforms for dialogue, trust-building exercises between government and civil society, and development of multi-stakeholder committees/advisory groups to better integrate the input from a diverse body of actors.
- Financial obstacles impeding their self-sufficiency (for example through funding strategies must be mitigated.
- Academia should encourage the engagement of people in Civil society debates and actions.

6.3 Providing capacity-building efforts

- Academia should propose interdisciplinary curricula and developp research project in the field. They have to break the traditional disciplinary silos.
- Dissemination of findings and best practices, and promotion of platforms for cross-fertilization with various disciplines, e.g., regarding development, conflict prevention, good governance and peace-building, human rights and women's participation.
- Further dissemination of findings and best practices by facilitating translation of publications into various languages.
- The Tech community should contribute to propose solutions that can enforce and promote peace and security ("security and privacy by design").
- To enforce cyberpeace's initiatives Academia should develop education and research in "cyber" taking into consideration the following responsibility issues:
    - Responsibility to protect the planet and life interests;
    - Responsibility to establish a secure, equal and durable international economy;
    - Responsibility for the safety, freedom and well-being of humanity.
    - Responsibility to enforce human rights protection in cyberspace and in real life.

6.4 Strengthening of Partnerships between government and civil society actors

- Roles and responsibilities must be clarified and delineated among governmental and non-governmental stakeholders.
- Expectations must be managed with respect to deliverables for all participants.
- Components best left to civil society actors should be identified, with responsibility for certain initiatives ceded to civil society without governmental interference.
- Academia should contribute to developp competence that can be useful in shaping norms.

6.5 Interplay between civil society and private sector actors

- Private sector investment in and collaboration with civil society efforts should be encouraged.
- Corporate social responsibility projects should be encouraged.
- Multi-stakeholder (whole of society) approach to online and offline counter messaging should be encouraged, particularly when leveraging the ICT sector in collaboration with and informed by other relevant civil society actors.
- Developp consummers expectations for more quality of e-service, more ICT's infrastrcutures robustness ans resilience.

- Enforce inititatives that ensure that Human rights are respected in cyberspace.
- Academia should encourage student to develop a cyberethic that can be effective when working for the private sector.

6.6 Media

- Media literacy and responsible reporting on cyber incidents and technological risks should be encouraged.
- Professional media and social media platforms should be encouraged and supported to improve media coverage.
- Training of journalists should be encouraged.
- Cyber incidents should be reported objectively.
- Critical thinking skills should be developped.

6.7 Questions for Discussion

Topic 1. What are the sources of legitimacy and authority of civil society (in the broad understanding of the term) in driving the debate? For example, when it comes to the implementation of 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'?

Topic 2. Should an attempt be made to organize 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?

Topic 3. How can civil society play a greater and more targeted role in promoting civilian oversight of national and international policy and strategy relating to ICT in the context of peace and security? More specifically, how can this kind of oversight be applied to the growing interest of States in offensive capabilities and operations?

Topic 4. Are there areas in which civil society should not seek to be involved, i.e., are there roles and responsibilities which civil society should perhaps leave to others?

6.8 Observation/Analysis distilled from the Workshop

As the Geneva Dialogue on Responsible Behavior in Cyberspace unfolded over the two-day workshop, it became clear that, while the views and perceptions of what constitutes responsible conduct differ depending from one stakeholder to the next[23], there appears to be a unity of purpose regarding the overarching goal, which is to maintain cyberspace as a shared environment that is open, peaceful, free, accessible and stable. Because cyberspace is an integral part of the current international (rules based) order, current geopolitical tensions are a constant reminder that these values must be protected. However, there is little common understanding regarding how open, peaceful, free and accessible can be defined, let alone how they can best be upheld.

This conceptual (ideological?) divide was noticeable when representatives of the various work streams (governments, private entities and civil society) expressed views on these features; however, the biggest disparities exist between liberal democracies and the more authoritarian countries. Participants

[23] "Lack of shared of understanding of what responsible behavior is, therefore this initiative is timely"; Reference made by Pablo Hinojosa

felt that this disconnect (gap?) between unity of purpose and the chosen path (towards an open, free, peaceful and stable cyberspace) was growing. This view was particularly strong in light of the rapid commercialization of digital economies from countries such as China, their dominance in the digital global market[24] and concurrent increases in Internet censorship[25]. Consequently, it is unlikely that a common understanding will be reached not only between states and other states, but even between states and non-state stakeholder groups. As Pablo Hinojosa commented "we don't foresee common understanding between the technical and state community".

In the context of international peace and security, it is advisable to conceptualize the technical community quite narrowly. For example, regarding the roles of network operators and Computer Emergency Response Teams (CERTs), network operators manage and monitor the networks and guarantee interconnections, while CERTs act as first responders.

The terms that define the target – *open*, *secure*, *stable*, *accessible*, and even *peaceful* – all require similar limitation. *Open* refers to "end-to-end" unrestricted access; *secure* implies resistance to attacks; *stable* means continuously and consistently available; and *accessible* means available without restrictions. For the last of these parameters, *peaceful*, it is difficult to provide a functional (technical) definition.

Regarding the distinction between *building* and *maintaining trust*, international relations operate on the assumption of very limited state-to-state trust, and thus making the concept of trust-building much more applicable. *Maintaining trust* pertains far more to the relationship between the technical community and society as a whole, as societal trust of the Internet as a medium for communication is the basic foundation of cyberspace relationships.

Disagreement as to the definitions of these terms became clear from other civil society representatives. It is important to note that, while states do have the primary responsibility to keep cyberspace stable, state-level actions have a direct impact on civil society groups and on human rights in general. Thus, while this normative framework for responsible (state) behavior is further developed, human rights will require increasing emphasis. Civil society organizations need to convene to articulate norms to define and develop norms that pertain to their specific fields and tasks[26]. Certain state-level behaviors, such as targeted surveillance of dissidents, directly undermine fundamental civilian freedoms. Furthermore, cyber "security" firms are marketing new types of technology – spyware – obviously designed to help governments and criminals infiltrate, monitor and possibly sabotage or otherwise manipulate civil-level computer systems.

Regarding such potential abuses, civil society organizations have clear roles with respect to awareness raising, education, capacity-building, accountability, transparency, and even diplomacy. Given the newness of the medium, it is understandable that their performance of these roles leaves considerable room for improvement. Still, their position allows them to draw attention to particularly vulnerable stakeholders and to provide trusted data. Furthermore, civil society is positioned to effectively "name and shame" dangerous state-level actors.

For the moment, though, no civil organization fulfills this role – that of a "Cyber Amnesty International". Civil society engages strongly in other security policy areas, such as autonomous weaponry or the nuclear domain. Why, then, is such engagement lacking in the digital realm? One possible explanation is the lack of participatory platforms to support civil society organizations' participation in state-centric multilateral negotiations.

---

[24] e.g., investment in digital technologies such as artificial intelligence, financial technology/fintech, virtual reality, autonomous vehicles, 3D printing, robotics, drones, etc.

[25] References made by Carmen Gonsalves

[26] References made by Jon Penney (Citizen Lab).

In this regard, workshop participants called attention to the ICT negotiations in the context of international peace and security currently taking place within the UN General Assembly's First Committee (for Disarmament and International Security) in New York. Both adopted resolution[27] have introduced language that will facilitate consultations with UN members outside the Committee as well as non-state actors.

Three aspects need to be considered in further developing the concept note:

1. Emphasis on the importance of Human Rights and of civil society groups;
2. Emphasis on defense and capabilities: It is particularly important to invest in defensive tools to make infrastructure more secure. Good practices and best societal security practices need to be identified in order to improve resilience and the defensive capacity;
3. Emphasis on business behavior: What impact do corporations/corporate-level entities have on human rights? The interplay between business behavior and human rights violations requires more research and attention from the international community.

Representatives of civil society encourage states to facilitate, support and fund fact-based/empirical research. Basic steps, including basic standards of cyber hygiene, need to be mainstreamed into everyday life. Phishing, for example, is a very basic kind of threat. As long as it works, i.e., as long as common people lack the necessary means to identify even such simple attacks, they will continue to be used by malicious actors.

One strong role civil society organizations fulfill is in enforcing agreed norms. To go a step further, civil society organizations need a venue via which to hold their states accountable for wrongdoings. To this end, it is recommended that they issue reports outlining, for example, how spyware is being abused by governments to track dissidents.

Reporting of this kind is vital both to individuals' awareness and to state-level actors' accountability concerning practices that undermine international peace and security. Of course, all documentation needs to be factual, research-based, empirically verifiable, and available for dissemination[28]. In the workshop, delegates from civil society organizations argued that holding states accountable and promoting research on state and non-state practices would require non-state actors to devote more resources to spreading awareness.

The EUISS[29] is currently running two projects:

1) Cyber capacity building guidance; and
2) the EU Cyber diplomacy initiative in order to support MS.

According to EUISS Brussels Executive Officer Patryk Pawlak, civil society organizations need to challenge their governments' views both more often and more aggressively. The two main implications of this assertion are first that civil society organizations' tend to accept and follow official narratives and trains of thought, and second that this tendency leaves them prone to disinformation and other abuses.

---

[27] The Russian resolution proposes the establishment of an Open Ended Working Group and suggests that non-state actors be consulted.
The American resolution proposes another UN GGE and suggests that regional security organizations and non-state actors be consulted. Another examples to hold consultations is the Fissile Material Cut-Off Treaty.

[28] For example: peer-review journals? That would be a venue for dissemination.

[29] European Union Institute for Security Studies https://www.iss.europa.eu/

What is more, non-state actors need to shape policy agendas regarding the development of an open, peaceful, secure and stable digital environment. Compared to governmental oversight offices, civil society organizations are well-placed to break silos and look beyond the usual suspects[30].

Occasionally, civil society organizations assume the task of safeguarding governmental and institutional memory. In doing so, they ensure continuity, not least because governmental organizations and institutions are often subject to personnel changes.

Civil Society Organizations such, do provide dedicated workshops on ICTs in the context of international peace and security in order to facilitate broader international participation. Conceived to empower countries from various regions, these capacity-building workshops focus on international law as well as cooperative confidence-building measures.

One participant stressed the importance of civil society organizations disclosing their funding sources, as this type of transparency increases non-state actors' credibility.

Unlike governments and private sector corporations, which are often the subject of criticism from civil watchdog groups, civil society organizations enjoy a high degree of confidence. In order to maintain this, they must provide verifiable, peer-reviewed findings and data on documented practices. Further, unlike businesses, their position implies an obligation to share their expertise and spread their acquired knowledge with others.

In performing the above tasks (awareness raising, education, capacity-building, accountability and Transparency) civil society organizations may need to assume adversarial roles by questioning and challenging government activities. However, it must be considered that states rarely welcome criticism; however, individual departments are often very protective of their standing in relation to others. Therefore, simply ranking governmental policies and their implementation might yield more positive results than naming and shaming the officials or departments behind them [31]. Also, depending on their philosophical bases, civil society organizations can compete with one another (e.g., advocating for policies and processes via letter-writing campaigns). Lastly, non-state actors can help implement useful policies by developing supportive tools and frameworks.

General Statements:

Civil society groups should do a better job in engaging actors from other regions, global south.

There are human rights reviews for internet protocols (IETF?).

More evidence-based research needed, which in turn depends on sustainable funding.

When providing technical information for the purpose of attribution, it is important to note that technical attribution is less important for technical community organizations than it is for governments.

The technical community can further help build strategies relating to CERT-to-CERT cooperation at a global level.

[30] The Quest for Cyber Confidence- ITU (2014)
https://www.itu.int/pub/S-GEN-WFS.02-1-2014
[31] Reference made by representative of Kenya.

7 Break-Out Session - Civil Society in Practice with respect to the UN GGE

7.1 UN

The 2013 UN GGE report was the first to acknowledge civil society's role in developing and implementing cooperative measures. In doing so, it opened a window of opportunity for civil society to engage in state-centric processes. The report of 2015 emphasized the importance of engagement at that level. The relevant passages of that report are reproduced below.

> **UN GGE 2015 (para 23):** In the interest of ICT security capacity-building, States may consider forming bilateral and multilateral cooperation initiatives that would build on established partnership relations. Such initiatives would help to improve the environment for effective mutual assistance between States in their response to ICT incidents and could be further developed by competent international organizations, including the United Nations, the private sector, academia and civil society organizations.
>
> **UN GGE 2015 (para 31):** 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.
>
> **UN GGE 2015 (para 32):** Areas where further research and study could be useful include concepts, relevant to State use of ICTs. The United Nations Institute for Disarmament Research, which serves all Member States, is one such entity that could be requested to undertake relevant studies, as could other relevant think tanks and research organizations.

In addition to these paragraphs, the norms listed in the UN GGE report 2015 allude to non-state actors' possible roles in fostering international cyber stability[32].

Participants of the breakout group agreed that in putting the issue of ICT, and in particular the UN GGE results on the agenda of governments across the world, education is paramount. Unfortunately, global awareness of the UN GGE process and its results is scant.

> **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

Research institutes and academia should help analyses what terms such as stability, international cooperation, cooperative measures, harmful activities, etc. means.

They could help hold states accountable if they lack to provide the structures and platforms to engage with other, non-state actors.

Civil society organizations can scrutinize state's activities and monitor state-to-state cooperation.

> **13b)** 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.

[32] Crespo L. (2018), Switwerland's contribution to international cyberstability, Phd. UNIL.

Private companies, academia and technical actors can help develop frameworks for attribution: what is needed to identify the perpetrator of a cyber-campaign (technical, legal and political considerations). Could non-state actors provide support in developing standards for proof?

> **13d)** 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.

The recommended exchange of information (e.g., reporting of incidents) could be improved with the help and involvement of public and private partnerships. Academia could further help develop templates to facilitate state-to-state cooperation.

Academic and civil groups could elaborate on the notion of terrorist use of ICTs, clarify what it implies and what it excludes, and provide overviews of ongoing and completed work (mapping).

Academia and civil society could help both to develop propaganda-identification measures and to determine ways to support individuals in distinguishing propaganda from reliable information, etc.

> **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.

How can academic, tech sector, civil society and individual actors contribute to the culture of cybersecurity?
Academia and civil society could help develop practical tools and guidance techniques, and describe basic measures to spread information on cyber risks, malware, etc. (Proposal: develop application to raise awareness, such as mobile Applications)

> **13i)** 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.

> **13j)** 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.

While helping civil actors develop frameworks to report and remedy ICT vulnerabilities, academic leaders could lead and mediate discussions on pressing issues: What constitutes responsible reporting? How could this be monitored by civil society? What rules of engagement should apply between private and public sector actors to illuminate and correct vulnerabilities?

> **13k)** 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.

The technical community could develop a sort of “rapid reaction plan” for those cases that CERTs are used to run cyber attacks on others. If that norm is violated, the technical community could rapidly react and document the activities.

It is crucial for the technical community to report on ICT-related vulnerabilities and back these documents with evidence-based research.

UN GGE 2013 (para 12): While States must lead in addressing these challenges, effective cooperation would benefit from the appropriate participation of the private sector and civil society.

IV. Recommendation on CBMs and the exchange of information

26d) Exchanges of information and communication between CERTs bilaterally, within CERT communities, and in other forums, to support dialogue at political and policy levels.

UN GGE 2013 (para 28). While States must lead in the development of CBM, their work would benefit from the appropriate involvement of the private sector and civil society.

V: Recommendations on capacity-building (para 31). In this (capacity building) regard, States working with international organizations, including United Nations agencies and the private sector, should consider how best to provide technical and other assistance to build capacities in ICT security and their use in countries requiring assistance, particularly developing countries.

7.2 General observations which were not addressed during the work-shop

General Considerations on Establishing a Cyber security Culture
From an end user's point of view, the first line of defense against malicious cyber activities is to understand the types and levels of risk they face. Unfortunately, while many individuals use ICTs, few fully grasp the security implications of the involved technologies. If more did, standard protective behavior would vastly reduce the likelihood of perpetrators obtaining sensitive information, e.g., via "phishing" scams. With this knowledge gap in mind, fostering a cybersecurity culture would enhance common understanding regarding, inter alia, cyberspace in general, the ICTs that underpin it, malware, attack vectors, vulnerabilities, etc. The development of a cybersecurity culture and best practice guidelines for all stakeholders will help achieve these goals.

Developing a global cybersecurity culture has been on the international agenda at least since 2004, when the UN General Assembly adopted resolution 58/199[33]. Such a culture must include measures to deal with "key economic, legal, and social issues related to information security [in order] to help countries get prepared to face issues and challenges linked to ICT deployment, uses and misuses."[34]
While raising awareness is a vital first step, simply advise end users to adopt safe and responsible ICT-related practices will do little to change their behavior. Specific programs will be necessary to train stakeholders, from policymakers to justice and police practitioners, managers, information technology professionals, and finally end-users (including children and the elderly)[35].
To begin with, at every level of their education and employment, end users should be trained in cybersecurity and basic cyber-hygiene. Developing an interdisciplinary approach to cybersecurity will be a

[33] United Nations General Assembly (2004). Creation of a global culture of cybersecurity and the protection of critical information infrastructures.
https://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_58_199.pdf
[34] S. Ghernaouti-Hélie - "Information Security for Economic and Social Development" UNESCAP – 2008 – Link http://www.unescap.org/icstd/policy/
[35] Global Cybersecurity Agenda, ITU (2008)
https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx

truly value-adding activity, as it will permit people to deal proactively with a broad range of cybersecurity issues; it will also demand lifelong learning. As cyber-threats (particularly state-sponsored ones) become more sophisticated and dynamic, professionals will need continuous training to defend against them[36].
In developing and designing a cybersecurity culture, two main challenges will be first to correctly distinguish relevant local, national or global issues, then to develop effective and locally-viable responses. While international cooperation can contribute tremendously to identifying and neutralizing global and generic issues, actions targeting local cultures require tailored local and temporal solutions.

The OECD's 2002 information system and network security guidelines, *Towards a culture of security*[37], focus first on awareness and responsibility. This acknowledges that individuals typically lack appropriate information to be effective and responsible cybercitizens. Awareness, knowledge and appropriate behavior are indispensable not only to prevent incompetent and naive errors but to develop trust and confidence in digital infrastructures, services and cybersecurity mechanisms.
Currently, most ICT end users (individuals or organizations) simply fail to understand cybersecurity issues and have neither the skills nor the tools to correctly protect their assets. As a result, they lack the objective means to adequately inform any confidence they may have in digital infrastructures and services. Therefore, they must rely on products and mechanisms they understand only poorly (if at all) and on solutions that have been imposed on them. The majority of these are designed with unreliable security and privacy measures.
Based on the issues discussed here, four essential security-building measures are recommended:

- Educate and train end users *via involvement of academia and civil society actors*
- Increase public awareness to enhance users' cybersecurity-related behavior;
    - Conduct awareness-raising campaigns targeting and supporting the general public in maintaining their personal cybersecurity.[38]
- Encourage cyber hygiene habits[39] (with assistance from academia and civil society)
- Develop awareness to support secure use of online devices. Academia and civil society could help develop simple tools that explain specific devices' risks and opportunities, as well as dealing with emerging vulnerabilities (e.g., via regular updates of web applications and digital tools).

The OSCE
OSCE Permanent Council Decision 1202 on confidence-building measures, which was adopted in 2016 to reduce the risks of conflict stemming from ICT use, does not explicitly mention civil society. However, **CBM 7** specifies that "participating states will voluntarily share information on their national organization; strategies; policies and programs – including on co-operation between the public and the private sector". Moreover, the OSCE guide on non-military CBMs stresses the importance of participatory civil society, particularly regarding CBM implementation . Also, one recommendation arising from the 2014 OSCE Chairmanship Event in Switzerland was that non-state actors be offered a platform to engage in state-centric processes. "Through the promotion of regular academic feedback," it was argued that academic and civil groups could "provide a neutral voice". That event's report also recommended explor-ing ways to continue dialogue with civil society, such as via annual exchanges and special meetings.

[36] Solange Ghernaouti; ITU Regional Cybersecurity Forum for Europe and CIS, Sofia, Bulgaria, 07-09 October 2008.
[37] http://www.oecd.org/sti/ieconomy/oecdguidelinesforthesecurityofinformationsystemsandnetworkstowardsacultureofsecurity.htm
[38] Global Agenda Council on Cybersecurity. 2016. WEF.
[39] http://www.thecommonwealth.org/sites/default/files/inline/CommonwealthCyberDeclaration_1.pdf

CBM 4: Participating States will voluntarily share information on measures that they have taken to ensure an open, interoperable, secure, and reliable Internet.

The participation and support of non-state actors will be essential to implement this recommendation.

Civil society involvement could help define what constitutes an open, interoperable, secure and reliable Internet (e.g., What does this imply? What perspectives are available regarding these concepts?)

CBM 7: Participating States will voluntarily share information on their national organization; strategies; policies and programs – including on co-operation between the public and the private sector; relevant to the security of and in the use of ICTs; the extent to be determined by the providing parties.

CBM 12: Participating States will, on a voluntary basis, share information and facilitate inter-State exchanges in different formats, including workshops, seminars, and roundtables, including on the regional and/or sub regional level.

With respect to such activities participating States are encouraged, inter alia, to:

- Conduct such activities in the spirit of enhancing inter-State co-operation, transparency, predictability and stability;
- Complement, through such activities, UN efforts and avoid duplicating work done by other fora; and
- Take into account the needs and requirements of participating States taking part in such activities.

Participating States are encouraged to invite and engage representatives of the private sector, academia, centres of excellence and civil society in such activities.
To fulfill these recommendations, Academia and civil society could for example, organize workshops, seminars and roundtables at all levels.

8 Perspectives

The issue of responsibility in cyberspace is a complex one. In the global digital ecosystem, civil society has a significant role to play in ensuring the complementarity and coherence of public and private approaches for people.

Since the first World Summit on the Information Society (Geneva 2003), civil society is a key player of an open international dialogue. More and more people are being trained and attentive to these issues of roles and responsibilities in cyberspace. The millenniums are now young adults. In addition, the number of people and organisations affected by cyber dysfunctions is increasing. The negative impacts of cybercrime, cyber activism, disinformation or cyber conflicts are rising. Nowadays, there are requirements for international and multilateral regulation, for a more integrative approach of confidence building measure in cyberspace, and for promoting cyber peace initiatives. Indeed, like land, sea, air or space, cyberspace is a common environment that must be shared and regulated and where civil society can become a major actor to help define, develop and enforce responsible behaviour in cyberspace. This could be effective, only if civil society is not manipulated by the strongest and the most powerful actors.