Submission by Sweden
to UNGA resolution 68/243 entitled
"Developments in the field of information and telecommunications in the context of international security", 12 September 2014

Executive summary

While the development of cyberspace generates almost limitless opportunities, **security concerns relating to the use of information technologies and telecommunications (ICTs) need to be properly addressed through** international cooperation.

National IT security strategy work in Sweden has evolved over time and a Swedish government inquiry is **currently working on a national strategy on cybersecurity.** The **Swedish Defence Commission** has recently made assessments relating to cybersecurity and cyber defence, stressing the need for an increase in Sweden's overall cybersecurity capabilities.

Sweden participates and contributes actively in various international cyberspace fora, while also seeking bilateral and regional dialogues on cyber-issues, including in the Nordic-Baltic region. Sweden has in particular focused on **promoting human rights** in cyberspace and the **multi-stakeholder model** for internet governance as well as the need for fundamental **principles to guide international surveillance activities**.

Sweden is advocating a **consistent EU cyber policy** based on the EU's fundamental values and interests. A key development was the adoption 2013 of the **comprehensive EU Cybersecurity Strategy**. Sweden was one of the initiators of **the Freedom Online Coalition**, a group committed to advancing internet freedom worldwide. For three consecutive years Sweden has hosted the **Stockholm Internet Forum,** a multi-stakeholder conference aiming to deepen discussions on internet freedom and global development. Sweden was among a core group of states that initiated the **UN Human Rights Council resolution 20/8** 2012, which affirmed that the same rights that individuals have offline must be protected online. In three consecutive years Sweden has introduced **joint statements in the UNGA First Committee** pointing out among other things the need to maintain a human rights and multi-stakeholder perspective when addressing ICTs and international security**.** Sweden has also contributed actively to the adoption of the initial set of **OSCE Confidence-Building Measures** to reduce the risks of conflict stemming from the use of ICTs and to increase transparency, stressing in particular the respect and promotion of human rights.

Global efforts should be made to **formulate core principles to guide the use of ICTs and international relations in cyberspace**; some tentative concepts are suggested below. The international community, including all stakeholders, should engage in practical collaboration efforts to strengthen cybersecurity which could include the establishment of a **voluntary set of rules of behaviour** or standards of international conduct in cyberspace. Global actors should work towards **developing confidence-building measures** to increase transparency and predictability, thus reducing the risk of misperceptions or conflict in cyberspace.

Sweden would like to make use of the opportunity to respond to UN General Assembly resolution 68/243 **(A/RES/68/243)** entitled "Developments in the field of information and telecommunications in the context of international security", in particular as regards views and assessments concerning the questions (a) through (d) contained in operative paragraph 3.

While being aware of the lack of precisely agreed international terminology in ICT related concepts, **Sweden will mainly use the term 'cybersecurity'** and related concepts, signifying efforts aimed at the preservation of the confidentiality, availability and integrity of information in electronic communications networks and IT systems. The term 'information security' is often used by implementing government authorities, standards organisations and business, etc., with generally the same meaning, although its scope is narrower and more technically oriented. Both these terms are accordingly used in national and international practice. There is however a **risk of confusion in using the expression 'information security' in an international policy context**, as it is also used by some countries and organisations as part of a doctrine that regards information itself as a threat against which additional protection is needed. For its part, Sweden joins those who do not recognise the validity of the term 'information security' when used in this particular context, since it could then be employed in attempts to undermine universal rights and freedoms, including attempts to legitimise further controls on freedom of expression and access to information beyond those agreed in the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights.

(a) General appreciation of the issues of information security

An **open, free, stable and secure internet used for peaceful purposes is essential for economic, social and political development** in the 21st century. Cyberspace issues and information technologies and telecommunications (ICTs) are rightly given increasing attention in international relations, with a growing number of actors addressing various aspects of this field, including norms of behaviour and confidence-building measures, the applicability of international law, human rights protection, economic growth and development, cyber capacity-building, and internet governance.

The opportunities of cyberspace and the use of ICTs are almost limitless, with the internet as a facilitator and infrastructure for socioeconomic activities as well as a catalyst for development, growth and innovation. An emergent and critical dependence on cyberspace and ICTs also brings complex and multi-layered vulnerabilities to society, either by accident or design, stemming from states or non-state actors. **Threats and security concerns need to be properly assessed and addressed** in international cooperation in order to secure the flow of information and avert disruptions to critical ICT infrastructure. Core objectives of such efforts include **safeguarding the availability, integrity and confidentiality** of data and information systems and the infrastructures that depend upon them.

International deliberations on cyberspace issues and the use of ICTs in an international security context need to continue evolving with the view of seeking greater common understanding and shared views of these issues globally. One noteworthy development in this regard was the **adoption on 24 June 2013 of a report by the UN Group of Governmental Experts** (UN GGE) on "Developments in the Field of Information and Telecommunications in the Context of International Security".

Sweden welcomes these efforts and the adoption by consensus of the report. The 2012-13 UN GGE made a **significant contribution towards building an effective framework** for international norms of responsible behaviour by states on the basis of existing international law and practical cooperative measures. We encourage the current UN GGE to continue this important work while fully taking some crucial principles and concepts into account.

Firstly, **security and freedom** in cyberspace go hand in hand. Proportionate and legitimate security measures should enable users to enjoy core values and rights on the internet and not restrict them. Secondly, security measures or other government actions in cyberspace **need to take account of the distributed and bottom-up approach** of the internet, and in particular a **multi-stakeholder model** for internet governance, involving states, private sector and civil society actors alike. Thirdly, cyberspace issues are **inherently transnational and borderless, requiring global cooperation** and common solutions. This underscores the importance of **developing international norms and principles for responsible** behaviour as well as expanding transparency and confidence-building measures. Key objectives include predictability, trust and stability in the use of ICTs, as well as accountability and legitimacy for the further development of cyberspace. Such efforts should be inclusive and pursued on the basis of existing international law and obligations.

There are **particular challenges in calibrating the appropriate role of states** in a global and public sphere of such rapidly growing importance to society as cyberspace, an area dominated and mainly developed by private actors and individual users. On the one hand it is evident that the success and impact of the internet relates directly to its decentralised, innovation-driven approach and organic evolution, mainly shaped by individual and private actors. On the other hand, as the role and use of the internet and cyberspace become increasingly important for societal development in general, states – as in any other public arena profoundly affecting society – have the obligation to uphold the rule of law, public safety and national security, and ultimately to protect society and its citizens. Neither complete political laissez-faire nor full state-control is a solution for the development and management of cyberspace.

(b) <u>Efforts undertaken at the national level to strengthen information security and promote international cooperation in this field</u>

A public inquiry mandated by the Swedish Government is currently working on **a national strategy on cybersecurity.** Presenting its findings on 1 December 2014, the ongoing inquiry will:

• **propose a national strategy** for the handling and transfer of information in electronic communications networks and IT systems;

• **propose overarching objectives** for efforts regarding cybersecurity and information assurance in society and how Sweden is to uphold security and privacy in IT infrastructure that is important to society as a whole;

• **define terminology** used in this area and, if necessary, propose clearer or alternative names and definitions, particularly with regard to terms used in the national strategy proposal; and,

• on the basis of its remit, **describe the responsibilities and roles of central government authorities** on the basis of their current tasks and mandates in the area of cybersecurity and information assurance.

While efforts to develop a national strategy are currently being pursued, **IT security strategy work in Sweden** has evolved over time. A strategy to improve internet security in Sweden appeared in 2006. There is also an operative strategy in place at government agency level, the *Strategy for information security in Sweden 2010-2015*. The Swedish Civil Contingencies Agency (MSB) has produced this strategy for societal information security in cooperation with the so-called *Cooperation Group for Information Security (SAMFI)*, a cooperative network of authorities with specific societal information security responsibilities as identified by the Government. The scope of the SAMFI cooperation includes strategy work, technical issues, standardisation, training exercises, management and prevention of IT

incidents and general national and international development in the field of information- and cyber security. To implement the objectives set up in the *Strategy for information security in Sweden 2010-2015*, an action plan has been developed, *Sweden's Information Security – National Action Plan 2012*. It primarily serves as a tool for the authorities in the SAMFI group to help in identifying priority measures. In 2011 the Civil Contingencies Agency (MSB) established the *National Cybersecurity Coordination Function* as a forum for situational awareness and collaboration. It focuses on prevention and coordination of incident response management, including cooperation with the Armed Forces to protect confidential information.

Cyberspace-related issues involve several government ministries in Sweden, including the Ministry of Enterprise, Energy and Communications, the Ministry of Defence, the Ministry for Foreign Affairs and the Ministry of Justice. A number of central government authorities under different government ministries have responsibilities in the field of cybersecurity and information assurance.

The basis for cybersecurity and information assurance work in Sweden is the **'principle of responsibility'** whereby an actor or government authority normally in charge of certain tasks retains the same responsibilities also during a crisis or incident. The background for this sectorial approach is that an actor with day-to-day knowledge of its own operations is considered most apt to deal with that particular area of responsibility during a crisis or contingency situation as well. Hence, government authorities in Sweden are responsible for their own IT security in accordance with relevant government regulations in the field. This modus operandi also entails an obligation to cooperate and coordinate with other relevant actors in preventing or handling serious incidents. For serious cyber crises affecting large parts of society, crisis management at central government level may need to be coordinated. The Swedish Civil Contingencies Agency (MSB) supports such coordination by providing methods and networks for the competent authorities during extraordinary events.

Relevant central government authorities with responsibilities in the cybersecurity field include:

The Swedish Civil Contingencies Agency (MSB), Office of Information Assurance and Cybersecurity has **coordinating responsibility for information security and cybersecurity** with regard to incidents that may affect several sectors. The MSB also support the Swedish Government Offices with situation reports in the event of serious crises or disasters, and provides methods for crisis communication and the coordination of official information to the public. MSB generally provides advice and support in a wide range of areas within the field of cybersecurity and information assurance, including guidelines, recommendations and awareness-raising material. At the Office of Information Assurance and Cybersecurity is the **Computer Emergency Response Team** (**CERT-SE**). CERT-SE is the national and governmental CERT of Sweden and is tasked with supporting the management and prevention of IT incidents and with increasing IT security awareness in society by supplying expert knowledge and assessments. The CERT-SE issues warnings and advice regarding vulnerabilities in IT systems and serves as the front end **national point of contact for equivalent services** in other countries.

The Swedish Post and Telecom Authority (PTS) is responsible for the **electronic communication sector as regards issues related to robustness, security, integrity and supervision**. The PTS also carries out inspections and issues regulations and guidelines.

The National Defence Radio Establishment (FRA) is the national authority for signals intelligence and the government's technical resource concerning **information security.**

The Swedish Defence Materiel Administration (FMV/CESEC) is the national certification body for IT-security based on the international standard ISO/IEC IS 15408, known as Common Criteria (CC).

The Swedish Armed Forces (FM) have certain responsibilities including **the IT defence unit and the Armed Forces CERT** and auditing. They also carry out inspections and issue regulations and guidelines.

The Swedish National Bureau of Investigation (RPS) investigates **computer-related crime and cybercrime** and has, for example, certain auditing responsibilities.

The Swedish Security Service (SÄPO) is responsible for **protective security measures, including cybersecurity with respect to national security**. SÄPO also carries out inspections and issues regulations and guidelines.

The Swedish Defence Research Agency (FOI) conducts **research on many aspects of cybersecurity**, and maintains a **Cyber Range and Training Environment** (CRATE) for experiments, competitions and exercises.

The Swedish National Defence College (FHS) conducts **strategic cybersecurity and cyber defence studies** and develops **educational high-level courses on information assurance** together with procedures and manuals on how to build technical cyber defence exercises (CDX).

The Swedish Data Inspection Board (DI) has certain responsibilities including auditing with regard to the protection of personal data and the **privacy of individuals in the information society**. DI also carries out inspections and issues guidelines.

The Swedish International Development Cooperation Agency (Sida) has ICT development related activities as one of its prioritized focus areas and works through support to global, regional and local initiatives in the field of policy and rule of law, strengthening and protecting human rights, and both civic and cyber capacity building. Sida addresses cyber security related issues from a human rights based approach, focusing on bottom-up initiatives for democratization and economic growth. This is being made both through initiated policy related work in normative processes, International Training Programmes (ITP) and directed support to a large number of actors across the world.

The Swedish Defence Commission addressing cybersecurity issues

The **Swedish Defence Commission** (*Försvarsberedningen*), consisting of parliamentarians representing all political parties represented in the Swedish *Riksdag*, has analysed international and regional developments, **drawing conclusions for Swedish security and defence policy**. The Commission addressed cybersecurity, among other issues, in its reports presented in 2013 and 2014. Some of the **assessments and proposals relating to cybersecurity and cyber defence** by the Defence Commission include the following:

- The transformative and constantly evolving nature of ICTs constitutes a **challenge to many of the traditional approaches in the field of national and international security**. Our societies' increasing dependence on ICTs and growing vulnerabilities in the global IT networks of today are, and will remain, one of our most complex and challenging issues for the future.

- As the development of ICTs as well as the management and ownership of IT networks are, to a large extent, in private hands, **collaboration between public and private actors** is seen as a key element in maintaining an effective and secure level in the management and use of ICTs.

- The **cyber field can be used as an instrument of coercion or force in state-to-state conflict**, on its own or in conjunction with other capabilities. The antagonistic use of cyber capabilities, such as computer and network attacks, can effectively restrict the room for manoeuvre of the target and be a **threat to national security and ultimately state sovereignty**. Computer and network attacks may cause effects similar to those of an armed attack by traditional means. To unambiguously **determine the origin, character or effects of such events** with sufficient certainty is a **complicated and potentially contentious matter**.

- The Defence Commission is of the view that **international law** – which is applicable in peacetime (including the United Nations Charter) and during armed conflict - **applies also in cyberspace**. There are however particular difficulties in maintaining a clear distinction between situations of peace and armed conflict in cyberspace. Public international law that may be deemed of relevance includes sovereignty, state responsibility, human rights, self-defence and the use of force.

- **International cooperation needs to evolve** in order to ensure a more robust cybersecurity environment. As a point of departure, such efforts should strive towards **international harmonisation of ongoing activities with other international actors**. There is clear added value in **deepening cooperation** among the **Nordic and Baltic states** with respect to these issues.

- As cyberspace is increasingly used for **industrial espionage**, which may constitute a security threat, all **actors need to increase their awareness and capabilities to protect** their activities. The Defence Commission underscores the significance of public and private actors in cyberspace having access to necessary enabling structures and associated regulatory frameworks to detect and handle various cyber events, including attacks.

-The Defence Commission **points out the need for an increase in Sweden's overall capabilities** to prevent and actively handle the impact of threats and attacks in the cyber field. In order to enable coordinated decision-making, the Defence Commission underlines the **need for shared situational awareness between civilian and military authorities** regarding particular cyber-related events.

- The Defence Commission has **stressed the need for further studies on threats and risks in the cybersecurity field**. Noting the decision by the Government to mandate a public inquiry on the development of a national strategy for the handling and transfer of information in electronic communications networks and IT systems, the Defence Commission reiterates the **need to consider strengthening IT robustness** in society and to study the **need to develop cyber capabilities**.

- Increased dependence on ICTs places high demands in the area of cybersecurity and information assurance in society on overall capabilities to resist different kinds of threats, attacks, incidents or interruptions of operations. The Defence Commission is of the opinion that **the Armed Forces, by virtue of their qualified cybersecurity capabilities, should be able to detect threats and assist and support relevant civilian authorities** as required.

In order to continue **promoting the development of cyberspace policies and capabilities**, Sweden is among other things working to forge international coalitions of likeminded states. Sweden has participated in and contributed actively to various **regional and international cyberspace-related fora**. These meetings and organisations include the so-called London process (cyberspace conferences in

London, Budapest and Seoul so far, with another scheduled in the Hague in 2015), IGF, ICANN, Freedom Online Coalition, EU, OSCE, Council of Europe, UNGA, UN GGE, EU, NATO, OECD, UNESCO, ITU, UNODC and international collaboration related to the Budapest Convention on Cybercrime. Sweden also seeks **bilateral and regional dialogues on cyber issues** with interested international partners.

Sweden has a longstanding international engagement in global cyberspace issues. In 2004 Sweden hosted an **International Expert Conference on Computer Network Attacks and the Applicability of International Humanitarian Law**. In recent years, Sweden has been a **leading advocate in promoting human rights and the rule of law** in cyberspace, particularly freedom of expression online, as well as the multi-stakeholder model for internet governance.

Sweden contributes substantially to **cyber capacity-building** efforts in low- and middle income countries through its international development cooperation, with an explicit focus on improving access to and increasing the use of open and secure ICTs through by means of improved infrastructure, regulation and institutions.

Within the EU, Sweden is advocating a comprehensive and consistent **EU cyber policy** based on the EU's fundamental values and interests. An important step in this regard was the adoption in 2013 of the **EU Cybersecurity Strategy** and the creation of the *Friends of Presidency Group on Cyber Issues* to address strategic, overarching cyber issues. This improved institutional framework enables the EU to more effectively contribute to the international debate and policy-shaping in cyberspace affairs. Sweden is also engaged in the negotiations on a directive concerning measures to ensure a high level of network and information security across the Union, which are currently taking place within the *EU Working Party on Telecommunications and Information Society*.

Sweden was one of the initiators of the **Freedom Online Coalition (FOC),** an coalition of governments committed to advancing human rights online. Since its inception in 2011 the coalition has grown from 15 to 23 member countries. FOC conducts yearly high-level meetings and issues joint statements and declarations.

The **Stockholm Internet Forum (SIF)** is an international multi-stakeholder conference initiated and hosted by Sweden, aiming to deepen discussions on how freedom and openness on the internet can promote economic and social development globally. It has been held in Stockholm for three consecutive years, for the first time in April 2012 and most recently on 27–28 May this year.

In close cooperation with a core group of states, Sweden initiated the **UN Human Rights Council resolution 20/8** in 2012, which affirmed that the same rights that individuals have offline must be protected online. The resolution was adopted by consensus and co-sponsored by 87 countries, giving it significant cross-regional backing. A follow-up resolution (26/13) was adopted without a vote on 20 June this year, reaffirming the main messages from the 2012 resolution while including important additions on human rights and security as well as the importance of internet access for global development and the right to education.

Sweden has contributed substantially to the preparatory process for the **follow-up of the World Summit on the Information Society (WSIS)** in both the **ITU and UNESCO**. With the final review of the WSIS process scheduled for the fall of 2015 in the UNGA, Sweden is working with all stakeholders to ensure that the WSIS process remains focused on ensuring that the efforts of the UN system are directed towards improving the contribution of ICTs towards achieving global development goals.

Sweden has also taken a strong interest in the work of the **UN Group of Governmental Experts on information and telecommunications in the context of international security** and its mandating UNGA First Committee resolution. In the last three consecutive years since 2011, Sweden has initiated joint statements in the UNGA First Committee pointing out, among other things, the need to maintain a human rights and multi-stakeholder perspective in an international security context. Last year's joint statement welcomed the efforts of the UN GGE and the adoption by consensus of its 2013 report, winning the support of 40 states, including members of the UN GGE.

Sweden has also contributed actively to the adoption of the **initial set of OSCE Confidence-Building Measures to reduce the risks of conflict stemming from the use of ICTs**, stressing in particular respect for and promotion of human rights in this context. Further efforts to develop and implement confidence-building and transparency measures are currently being pursued within the OSCE. Sweden submitted preliminary information regarding its initial implementation measures ahead of the capital level meeting of the OSCE Informal Working Group on cyber confidence-building measures held on 15 May 2014.

With respect to issues related to **international surveillance activities**, at the Seoul Conference on Cyberspace in October 2013 Sweden outlined **seven fundamental principles** that should be observed by all states to fully assure the legality and legitimacy of any surveillance, while safeguarding the rights of individuals. Sweden will continue to seek a dialogue with all stakeholders based on these principles.

Nordic regional cooperation on cyberspace issues is increasing, including in the foreign and security policy field. The **Nordic countries and the Baltic States (NB8) as well as other likeminded countries** meet on a regular basis to discuss cyberspace issues.

The MSB Office of Information Assurance and Cybersecurity (CERT-SE) participates in the **Nordic National CERT cooperation (NCC)** and cooperates closely with counterparts in the Nordic region and other countries. The Nordic National CERT Cooperation was established in 2013 and is employed by the national CERTs to increase protection against IT incidents and cyber-attacks.

Sweden regards the **Council of Europe's Budapest Convention on Cybercrime** as an essential element of the global framework for measures to combat information network crimes The government has on several occasions expressed its clear intention to ratify the Convention. Several legal assessments and a broad consultation procedure regarding required national measures in order to fully comply with the Convention have been made. The next step is to prepare a legislative bill for Parliament. While ratification will not be possible before 2015, it should be noted that Swedish law already meets the majority of the requirements of the Convention, including for instance the so-called 24/7-network which was established in Sweden many years ago.

Sweden cooperates with **NATO in the framework of the Partnership for Peace Programme (PfP)** and participates in some NATO working groups and exercises in the cyber defence field that are open to partners. There are currently efforts towards further collaboration as Sweden is in the process of applying as a contributing participant to the **NATO Cooperative Cyber Defence Centre of Excellence**.

(c) **The content of the concepts mentioned in paragraph 2**

Under this heading Sweden would like to state the following with respect to **international efforts "…aimed at strengthening the security of global information and telecommunications systems…"** as contained in operative paragraph 2 in UNGA resolution 68/243 entitled "Developments in the field of information and telecommunications in the context of international security".

Acknowledging the evolving impact of ICTs in international politics and an apparent global trend to address and embed cyber issues in the existing framework of state-to-state relations and the application of international law, **core principles to guide global action in cyberspace** towards an open, free, stable and more secure cyberspace where fundamental rights are protected should be developed. While the list that follows makes no claims to be either exhaustive or complete, such core principles could include the following concepts:

1. **Adherence to existing international law, norms and obligations**. Existing international law and norms of state behaviour are essential and applicable in the use of cyberspace. Given the unique characteristics of the use of ICTs, however, further consideration and study may be required on how individual rules and principles apply in cyberspace. Efforts of the international community should at this stage focus on developing common understandings on the application of existing international law and the development of relevant norms of behaviour

2. **Human rights and the rule of law apply fully and equally online as offline**, as has been affirmed by the UN Human Rights Council. It is a basic understanding that the same rights that individuals are guaranteed offline must also be protected online, in particular freedom of expression, including the freedom to seek and impart information, as well as the right to privacy.

3. **Discussions on Internet governance issues should take an inclusive multi-stakeholder approach**. Mirroring the distributed character of the underlying technology of the internet and the dominance of private sector-owned and -managed IT infrastructure, discussions with wider implications for the future of cyberspace – in particular internet governance – should include all stakeholders: state, private sector and civil society actors alike from both developed and developing economies. Unwarranted changes that reduce or exclude the role of non-state stakeholders may be damaging to an accessible and interconnected internet, potentially curtailing a core driver of globalisation, innovation and prosperity.

4. **States are leading international security actors and, as such, accountable**. As the predominant, traditional security actors in the international arena, states also bear primary responsibility for security, safety, and enforcement in cyberspace, in accordance with, and accountable under, international law. States' extension of sovereign authority into cyberspace must be consistent with international law and all international obligations, including human rights and the fundamental freedoms of individuals.

5. **Cybersecurity need to be based on a holistic security concept.** A comprehensive security concept in a modern and globalised world cannot exclusively be regarded in terms of a nation-state sovereignty perspective, but also needs to include a clear focus on individual rights and human aspects of security. Security is necessary in order to guarantee our basic democratic values, the functioning of society and the freedoms and rights of individuals. This should also apply to cybersecurity, as freedom and security on the internet are mutually dependent and reinforcing rather than conflicting.

6. **Cybersecurity needs to be technically neutral and not regulate information or content.** Regardless of the exact scope of a comprehensive definition of cybersecurity, controlling or restricting online information *content* cannot be explicitly or implicitly included in a concept of cybersecurity on the basis of the rule of law and international law. Security measures in cyberspace must be neutral and geared towards preserving the key technical internet properties

and characteristics (including open and global accessibility, integrity, resilience, and decentralised, innovative technical evolution).

7. **State surveillance activities in cyberspace need to be based on a principled and law-based approach**, subject to regulatory legislation and oversight adopted in a democratic and procedurally correct manner. In addressing international reactions to privacy issues, there is a need for an international dialogue on norms that should govern state surveillance operations on the internet. Such an approach would in particular have to be based on legitimacy, necessity, proportionality and transparency.

8. **State actions in cyberspace should not threaten or undermine stability and trust** in shared global ICT resources and should avoid incidental or unintended damage, particularly to critical information infrastructures. Concerns among the international community regarding the need for transparency and confidence-building measures should be adequately addressed by states acting in cyberspace.

9. **National laws and international agreements should increase rather than constrain the potential of cyberspace for innovation and experimentation** in the commercial, political, and social fields. All states should benefit from cyberspace as a central vehicle in promoting global economic development and growth, with particular emphasis on the developing world, bearing in mind the crucial role of private actors and markets in the development of technology, operations and commerce.

10. **Agreements on rules, conduct and institutions for cyberspace must be representative and created on the basis of reciprocity, accountability, and equality**, while respecting international law and human rights, and taking the multi-stakeholder character of the internet into account.

(d) <u>Possible measures that could be taken by the international community to strengthen information security at the global level</u>

In parallel to seeking global agreement on core principles to guide the use of ICTs and international relations in cyberspace, the international community, including all stakeholders, should engage in **practical collaboration efforts** aiming towards, inter alia:

- establishing an international **normative framework of acceptable State behaviour** based on existing international law and principles, including the establishment of a voluntary set of rules of behaviour or standards of international conduct in cyberspace;

- agreeing on and implementing both **traditional and innovative measures to strengthen cybersecurity** on the basis of international law and the rule of law while protecting and upholding human rights, including freedom of speech and privacy, intellectual property rights, as well as the availability, confidentiality, integrity and authenticity of data and networks;

- developing **confidence-building measures** to increase transparency and predictability and thus reduce the risk of misperceptions, unintended escalation or conflict in contingency situations;

- **exchanging national strategies and perceptions**, best practices and views on relevant international legal norms in the field;

- **establishing national CERTs** and situational awareness as well as notification of relevant contact points;

- **conducting joint exercises** to improve voluntary cooperation in joint incident-handling;

- working towards an **improved use of commonly agreed standards and legal approaches**, thereby strengthening international collaboration and **enhanced international capacity to tackle all forms of cybercrime**, including efforts to **promote the Budapest Convention on Cybercrime**;

- **enhancing dialogue** nationally as well as internationally **with other stakeholders**, including business and civil society, in keeping with the open, global multi-stakeholder nature of the internet; and,

- **protecting and strengthening the security, resilience and robustness** of critical infrastructure and **supporting cybersecurity capacity-building globally,** and in particular in developing countries.