# DELHI COMMUNIQUÉ ON A GFCE GLOBAL AGENDA FOR CYBER CAPACITY BUILDING

**24 November 2017**

GFCE
Global Forum on Cyber Expertise

# Delhi Communiqué on a GFCE Global Agenda for Cyber Capacity Building

## 24 November 2017

The Global Forum on Cyber Expertise (GFCE) is a global platform for countries, international organizations and private companies to exchange best practices and expertise on cyber capacity building. Its aim is to identify successful policies, practices and ideas for cyber capacity building and amplify these on a global level. Together with partners from non-governmental organizations (NGOs), the technical community and academia, GFCE members develop practical initiatives to build cyber capacity.

1. We, the members[1], partners[2] and advisory board of the Global Forum on Cyber Expertise (GFCE), use the opportunity of the Global Conference on Cyberspace 2017 in New Delhi, India, to announce a GFCE Global Agenda for Cyber Capacity Building, which derives from best practices and lessons learned in the development, security and technical communities.

2. We acknowledge other relevant outcome documents such as the 2030 Agenda for Sustainable Development (70/1); the UN General Assembly Resolution on ICT for Development (71/212); the UN Human Rights Councils Resolutions on the promotion, protection and enjoyment of human rights on the Internet; the World Summit on the Information Society (WSIS+10) outcome document (70/125); the UN General Assembly Resolutions on the Creation of a Global Culture of Cybersecurity (57/239, 58/199, 64/211); the recommendation of the 2016 World Development Report on Digital Dividends; and the Reports of the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, including the July 2015 Report (A/70/174).

3. We reiterate that strengthening confidence and security in the use of information and communications technologies (ICT) for the development of information societies and the success of and innovation in such technologies are drivers for economic and social prosperity.

4. We reaffirm that efforts to address security in the use of ICT will be consistent with international law, in particular the Charter of the United Nations, and respect the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights and the UN Guiding Principles on Business and Human Rights, where appropriate.

5. We reiterate that international cooperation and assistance play an essential role in enabling societies to secure their networks, ensure the free flow of information, and combat cybercrime.

6. We underscore that inclusive international collaboration and investment to ensure a free, open and secure cyberspace continue to play an essential role in enabling states to help secure ICT and acknowledge the positive contributions to cyber capacity building made by all stakeholders – including governments, international organisations, private companies, civil society, technical community and academia – within and outside the GFCE – in alignment with the 2015 Hague Declaration on the GFCE.

7. We reaffirm the overarching goal of the GFCE is to be a pragmatic, action-oriented and flexible forum that strengthens cyber capacity and expertise globally.

8. We reaffirm the GFCE's firm, shared commitment to strengthen cyber capacity and expertise globally and to make cooperative efforts by all stakeholders in this field more effective by advocating for the use of international standards and good practices, complementing, but not limited to, existing initiatives, and fostering collaboration across all stakeholders.

---

[1] African Union, Argentina, AT&T, Australia, Austria, Bangladesh, Belgium, Canada, Chile, Cisco Systems, Commonwealth Telecommunications Organisation (CTO), Council of Europe (CoE), Economic Community of West African States (ECOWAS), Estonia, European Union, Europol, Finland, France, Germany, Hewlett Packard, Huawei, Hungary, IBM, India, INTERPOL, International Association of Prosecutors (IAP), International Chamber of Commerce (ICC), International Telecommunication Union (ITU), Israel, Japan, Kenya, Latvia, Mauritius, Mexico, Microsoft, Morocco, NRD CS, The Netherlands, New Zealand, Norway, Organization for Security and Co-operation in Europe (OSCE), Organization of American States (OAS), Peru, Philippines, Republic of Korea, Romania, Rwanda, Senegal, Singapore, Spain, Suriname, Sweden, Switzerland, Symantec, Tanzania, Tunisia, Turkey, Ukraine, United Kingdom, United States of America, Vietnam, Vodafone, World Bank.

[2] DiploFoundation, Forum of Incident Response and Security Teams (FIRST), Global Cyber Security Capacity Centre (GCSCC), Meridian community, New America, United Nations Office on Drugs and Crime (UNODC).

**Key Themes of the GFCE Global Agenda for Cyber Capacity Building**

9. We commit to address the following capacity building themes in our efforts to build the capacity for good cyber practices internationally. This Agenda serves as a reference point for important themes and national capacities that are mutually reinforcing. This is not an exhaustive list of all the capabilities a country or organization needs to build its desired level of cyber resilience.

GFCE Global Agenda for Cyber Capacity Building

Theme 1. Cyber Security Policy and Strategy

a. Seek national level policy commitment to cyber security that drives strategic planning, resourcing and implementation.
b. Assess current national practices, threats and vulnerabilities, and develop, implement and evolve over time, as necessary, a comprehensive national cyber security strategy that considers how these issues impact all stakeholders and their respective roles in the process.

Theme 2. Cyber Incident Management and Critical Infrastructure Protection

a. Develop a national incident response system to prevent, detect, deter, respond to and recover from cyber incidents.
b. Develop, test and exercise emergency response plans and procedures, domestically and internationally, to raise awareness and ensure that government and non-government collaborators can build trust, prepare for, coordinate effectively and handle crises.
c. Identify and protect national critical information infrastructure sectors.

Theme 3. Cybercrime

a. Enact and enforce a comprehensive set of laws, guidelines, policies and programmes relating to cybercrime in line with existing international standards that allow for effective international cooperation, such as the Budapest Convention on Cybercrime.
b. Modernize and strengthen domestic criminal justice systems to deal with cybercrime and crimes involving electronic evidence, including the effective prevention, detection, investigation, prosecution and adjudication of such crimes in all their forms.

Theme 4. Cyber Security Culture and Skills

a. Promote comprehensive awareness across all stakeholders of cyber-related threats and vulnerabilities and empower them with the knowledge, skills and sense of shared responsibility to practice safe and informed behaviours in the use of ICTs.
b. Involve all stakeholders to create a workforce with a set of cyber security skills and knowledge employers require.

Theme 5. Cyber Security Standards

a. Promote the development and use of globally relevant cyber security standards that are developed in a consensus-based manner in bodies that are transparent and open to participation by all interested stakeholders and that enable achieving risk-based approaches to cybersecurity.

**Principles guiding the implementation of the GFCE Global Agenda for Cyber Capacity Building**

10. Recognising the importance of cross-cutting capacity issues, we encourage countries to conduct cyber capacity building in ways that take account of:
    a. the need for participation by all stakeholders in strengthening cyber capacity building;
    b. the need for treating the protection of critical information infrastructure and cyberspace as a shared responsibility that can best be accomplished through collaboration among all relevant stakeholders;
    c. the value of international cooperation;
    d. the necessity for fostering local expertise by using and creating regional expert hubs as capacity building multipliers;

e. the importance of information sharing by all stakeholders;
f. the benefits of cyber security research and innovation;
g. the multidisciplinary nature of cybersecurity, and the diversity of skills and knowledge required; and
h. capacity building's support to international security, including the applicability of international law, agreed voluntary norms and confidence building measures.

11. In support of stronger capacity building co-operation we endorse the following shared principles (inspired by the Global Partnership for Effective Development Cooperation[3] , and applied to cyber capacity building) – consistent with our agreed international commitments on human rights, decent work, gender equality, environmental sustainability and disability – for cyber capacity building:
    i. *Ownership*: nations need to take ownership of capacity building priorities focus on sustainable developments;
    ii. *Sustainability*: obtaining sustainable positive impact should be the driving force for cyber capacity building;
    iii. *Inclusive partnerships and shared responsibility*: effective cyber capacity building requires cooperation among nations, through a multistakeholder approach;
    iv. *Trust, transparency and accountability*: transparency and accountability play a key role in establishing trust, which is necessary for effective cooperation.

12. We encourage all relevant stakeholders to allocate funding and expertise for capacity building, applying the above principles and coordinating their support with other capacity building initiatives.

**Commitments**

13. We commit to the following actions in an effort to enhance our cyber capacity building:
    a. Seeking to mobilise additional cooperation, funding and support for cyber capacity building.
    b. Promoting the application of the Agenda and pursuing a results-based and action-oriented approach by the GFCE for the themes in order to:
        i. develop and promote good practice;
        ii. identify knowledge, technology and expertise gaps in our response;
        iii. narrow the gap between nations' cyber capacity building needs and the available resources;
        iv. avoid duplication of effort given limited resources;
        v. identify ways for increasing cooperation with the private sector and civil society in cyber capacity building;
        vi. mapping of global and regional progress in building the necessary capacities; and
        vii. share information among stakeholders in a timely and effective manner.

    c. Increasing efforts to expand the membership of the GFCE, for mutual benefits, and to garner the maximum number of members and partners.
    d. Collaborating with and encouraging relevant stakeholders to prioritise cyber security on their agenda and to contribute to cyber capacity building within their areas of expertise.
    e. Using the annual high level meeting of the GFCE to examine progress in the implementation of the Agenda and outline work plans for the year ahead.

[3] The Fourth High Level Forum on Aid Effectiveness (Busan, Republic of Korea, 29 November to 1 December 2011) articulated a number of principles for effective development cooperation in the Busan Partnership for Effective Development Cooperation.