The Geneva Initiative on Capacity Development in Digital Policy

We live in the midst of a digital transformation and are on the eve of even greater changes happening to society, driven by technological developments. Innovation is accelerating at an exponential pace. Artificial intelligence (AI), robotics, augmented reality, and big data make science fiction our social reality. New technologies will create new opportunities at the same time as they create new risks for society.

The *Geneva Initiative on Capacity Development in Digital Policy (the Geneva Initiative)* promotes innovative capacity development solutions to embrace digital opportunities and mitigate the risks.

The Geneva Initiative is the result of the Geneva Digital Talks (October - December 2017), online discussions in which stakeholders continued the policy-related dialogue, and research on digital policy. The Geneva Initiative relies on DiploFoundation's 25 years of experience in capacity development in digital diplomacy and policy, Internet governance, and cybersecurity. The Geneva Initiative will benefit from the experience and expertise from core partners such as the University of Geneva and the EPFL.

The Geneva Initiative focuses on the main needs for capacity in digital policy, and proposes ways to address these needs. While building on the unique expertise concentrated in the Geneva Lake Area, the Geneva Initiative aims to further build on and acknowledge, the excellent work done by organisations and initiatives such as the Global Forum on Cyber Expertise, the International Telecommunication Union, Internet Society, ICANN, and the Schools on Internet Governance.

For participation in the *Geneva Initiative* and additional information, please consult Dr Jovan Kurbalija, Head of the Geneva Internet Platform (jovank@dipomacy.edu) or Mr Michael Kleiner, State of Geneva (michael.kleiner@etat.ge.ch).

I) Capacity development in digital policy: Needs and responses

1. Building awareness about the digital transformation

Awareness is a pre-condition for effective digital policy. Awareness of the impact of technology on society should be developed among policy makers, international organisations, business representatives, media, civil society activists, the technical community, and citizens.

Recommended Activities: providing regular briefings for policy makers; promoting informed and dynamic media coverage; development of engaging video materials and infographics aimed at audiences with different levels of expertise in digital field; delivering regular updates on policy developments for policy makers, information specialists and general public.

2. Promoting technical solutions for cyber policy problems

The more cyber politics becomes controversial and divisive, the more relevant are practical technological solutions for cyber problems. For example, political discussion on attribution of cyber attacks could become more practical if there are reliable tools and means to identify sources of cyber attacks.

Recommended Activities: facilitating dialogue among technical, security, and policy communities on specific cybersecurity challenges; sensitising technical and policy communities about each other's work through consultation processes and online exchanges; promoting success stories about the effective use of technological solutions to address cyber policy problems.

3. Dealing with silos in digital policy

Digital policy issues are addressed in numerous and increasingly isolated silos: technological, economic, legal, and security, among others. Silos are a problem because digital issues are multidisciplinary; policies developed in silos will be less effective as they will not take into account the full range of related issues (human rights, economic, technological, etc.).

Recommended Activities: promoting a 'cross-silo-by-design' perspectives among actors aimed at ensuring that events wide representation of perspectives (i.e. participation of government representatives, civil society, business, end-user communities, technologists, and academics – in particular lawyers and economists – in e-commerce debates); supporting 'boundary spanners' – who can understand more than one professional context – who can work across silos; developing cross-silo dictionaries to ensure that terminology is not a barrier for communication among different silos.

4. Providing more evidence and data for addressing Internet challenges

Currently available data on the nature and impact of cyber issues on society is insufficient. For example, there are a wide range of estimates of the impact of cybercrime on the economy. Conflicting or insufficient data provides a poor basis for policy decisions.

Recommended Activities: developing institutional capacities for monitoring, collecting and processing data; enhancing academic and policy research related to metrics; facilitating communication between academic and expert communities and policy-makers; implementing existing and developing new indicators for digital developments.

5. Developing comprehensive institutional capacities for digital policies

Capacity needs to be understood at various levels: while training often results exclusively in the building of individual competencies (skills and know-how), capacity development aims at creating a sustainable impact on organisations and networks. From local to global levels, institutions need to leverage and coordinate individual skills, so they translate into organisational knowledge, expertise, procedures, and policy instruments to deal with issues such as cybersecurity, artificial intelligence (AI), and digital commerce. Failing to do so would reinforce a siloed approach to problem-solving and generate sub-optimal solutions, which only partially tackle the issue.

Recommended Activities: developing a holistic and whole-of-government approach for cyber policy by involving all relevant public institutions and stakeholders; facilitating, on request, the further development of the capacity of institutions that should contribute to developing international agreements, norms, and rules, and, on request, facilitate their implementation nationally; increasing 'vertical policy coherence' by enhancing cooperation between the UN and regional instances, such as for cyber norms and confidence building measures; providing training for diplomats and other governmental officials.

6. Ensuring access to justice in online disputes for citizens, businesses, and organisations

The global nature of the Internet, with users and servers spread across jurisdictions, and non-harmonised legislation across countries, makes dispute resolution complex, timely and expensive. Citizens, businesses, and organisations need ways to access justice in online disputes ranging from enforcing contracts in e-commerce to prosecuting cybercrime attacks.

Recommended Activities: mapping the main dispute resolution mechanisms, ranging from traditional (courts, arbitration) to innovative solutions; organising brainstorming sessions with experts from dispute resolution and online communities; running stress-tests for innovative dispute resolution via simulation exercises (possible introduction into teaching of universities and academic institutions); encouraging the development of cyber legal

clinics aimed to help citizens and organisations protect their rights online, ranging from enforcing contracts via protection of privacy to libel cases.

7. Strengthening capacities for responding to cyber-attacks

Cyber-attacks are becoming increasingly sophisticated. Vulnerabilities of digital systems, underpinning each segment of our society, are being exploited by individuals, criminals, terrorists, and political groups, as well as states. Consequences – economical, political, and even humanitarian − can be significant. Prevention and responses requires cross-sectoral cooperation. Organisations, companies, countries, and international organisations need capacity for timely and effective cyber-incident responses.

Recommended Activities: improving capacities for technical, legal, and diplomatic mechanisms to address requests for cross-border cooperation and dialogue in case of attacks; building monitoring, response, and mitigation capacities based on communication and cooperation between national and international entities and stakeholders; organising national, regional, and international exercises, simulations, drills, and table-top exercises with a multistakeholder nature, to develop, test and exercise emergency response plans and procedures.

8. Promoting shared responsibilities of governments, businesses, and users for cyber stability and digital developments

Promoting clarity with regards to the responsibilities of the main stakeholders (government authorities, the private sector, the technical community, civil society, and citizens) is essential for the development of stable and effective digital policies. When responsibilities are not clear and acknowledged by all parties, gaps may emerge. Where no stakeholder is taking action, or where there areas of overlapping responsibilities, confusion may be created.

Recommended Activities: conducting research on roles and responsibilities in various areas of digital policy, especially cybersecurity; facilitating cross-stakeholder discussions on how each party sees its own and others' roles and responsibilities

9. Leaving no one behind in the digital transformation of modern societies

Digital developments may amplify existing divides and create new ones, such as barriers to access online marketplaces and cybersecurity solutions. Vulnerable groups are particularly at risk of being left behind. Among others, people with disabilities, indigenous communities, poor and socially marginalised communities, as well as those who do not

speak dominant languages, need new capacities to participate actively in the digital realm.

Recommended Activities: monitoring digital divides; developing new policies that will promote the interests of vulnerable groups; developing the capacities of vulnerable communities to participate, in order to promote and protect their interests in digital negotiations; promoting the development of content in different languages; ensuring effective and inclusive online participation at major policy-shaping fora.

10. Working towards ethical responses to digital challenges

Society is searching for answers to the numerous questions triggered by technological growth. The ethical development of technology-based societies − respecting human rights and putting humanity at the centre − depends on working towards answers to some of these questions. In particular, artificial intelligence opens basic questions on the essence of humanity and its interplay with technology.

Recommended Activities: engaging philosophical and social academic departments in research on the ethical aspects of digital developments; organising ‘digital cafe philo’ events that address questions such as protection of core human values in the digital era and the impact of AI and other developments on free will and freedom of choice; developing new language and terminology for dealing with ethical and philosophical challenges posed by AI and other new technologies.

II) Approaches and methods for capacity development in digital policy

The *Geneva Initiative* promotes innovative capacity development which moves beyond training provision towards a more holistic and comprehensive approach, ensuring sustainable and effective digital growth in accordance with the spirit of Agenda 2030. The *Initiative* proposes the following approaches and methods to develop and implement inclusive, enabling, and sustainable digital policy capacity development,

1. Think global but act - and own - local

The Internet is a global system, however for communities worldwide, it is the local impact of the Internet which is important. The starting point for the *Geneva Initiative* is what International Geneva can offer through training, research, and policy development. The *Geneva Initiative* invites others to reflect on what they can do in their respective communities. Local action should address local needs, based on the local context. It should build local ownership of capacity development activities, which increases the effectiveness and sustainability of the results.

2. Respond holistically to digital transformation

Digital transformation - the increased digitisation of institutions, industrial sectors, and the growing social dependency on digital technology - requires a holistic and interdisciplinary response. For example, data - as the 'oil of the 21st century' - has technological, business, legal, security, and human rights aspects. One cannot address data as the core of the global economy without taking into consideration security or human rights issues, such as data protection. Any digital policy issue encompasses multi-disciplinary perspectives.

3. Involve a wide range of actors

Training and informal brainstorming events should adapt a smart multistakeholder approach, bringing together actors who could benefit from understanding each other's perspectives and developing personal relations. This inclusive approach applies to different stakeholders, but also to actors at different levels, from the international to the local.

4. Respond quickly, but think long-term

Pressing needs require quick action. Training, research, and policy dialogues are initial ways to address these needs. However, substantive and sustainable capacity can only be developed over time. Individuals and institutions cannot internalise new skills and develop

new procedures overnight. Activities aimed at long-term impact require planning, flexibility, and resources, including financial commitments.

5. Start with individuals, but aim to develop institutions

Currently, most capacity development endeavors in the digital field focus on training individuals. Competent individuals form a solid basis to develop institutions, which should be the next important step in capacity development. Functional and effective institutions are key to ensure sustainable and innovative digital development in countries and communities, both in the developed and developing world.

6. Address current needs, build on existing capacities, but keep the wider picture in mind

Capacity development which effectively addresses concrete and immediate needs, and builds on existing capacities, will capture the interest and active engagement of the people involved. For example, this might involve efforts to help officials develop a national cybersecurity strategy, to prepare diplomats to negotiate cybersecurity instruments, or to help small start-ups navigate complex data protection policies. However, while responding to immediate needs, it is important not to miss the wider perspective, and to keep in mind longer-term capacity needs and priorities.

7. Perform a ‘humanity check’ for capacity development

Since new technology - such as AI - may challenge some of the core values of humanity, capacity development should have a ‘humanity check’ aimed at ensuring that training, research, and policy activities promote the enabling and creative potential of technology, while containing its threats.

8. Move beyond technology towards society and economy

Currently, most capacity development in the digital field focuses on building technical skills rather than conceptual knowledge or soft skills. The next phase in capacity development should reflect the evolution of the Internet from a mainly technological system to the main agent of economic, social, and political change in today’s world.

From the current focus on technical training, digital capacity development needs to move towards conceptual knowledge and soft skills for business people, government officials, academics, philosophers, and other technical and non-technical professions. Soft skills might include intercultural communication, negotiation, and the ability to adapt and learn, to innovate, and to respond to the changing environment.

9. Remain flexible and ready to adapt to the unknown

Digital developments involve many ‘unknown unknowns’. We do not know whether AI will become - as Stephen Hawking said - ‘the best, or the worst thing ever to happen to humanity’. Capacity development should be flexible enough to adjust to changes that cannot yet be envisaged. While we all agree that technology should serve humanity, the way in which it should serve and what society will request will need to adjust very fast.

10. Establish trust through transparency and accountability

Trust is a necessary component for effective cooperation; cooperation is essential for capacity development in digital policy. However, trust may be difficult to establish when working across different policy fields and institutions. Yet, trust can be built through transparency and accountability. The digital policy community should work towards a safe environment for sharing expertise, resources, and unique achievements and innovations, while recognising individual interests.