Contribution to the Global Digital Compact

Submission to the Thematic Area "Digital commons as a global public good": A systematic, whole-of-society approach to digital security.

For years, the international development community has put great efforts into digitalization as an opportunity to fight poverty. Like the revolutions that preceded it, the Fourth Industrial Revolution has the potential to raise global income levels and improve the quality of life for populations around the world. However, digitalization also provides a new breeding ground for organized crime. Thus, a new dimension of social vulnerability follows in the wake of the development opportunities offered by the digital revolution. In order to be sustainable, digital development must be done with a focus on digital security.

As more people and devices are connected, the risks that come with cyber insecurity will only increase. While significant past efforts have improved our risk posture, viable solutions are typically only available at a high cost, thus reserved to larger companies and the wealthiest governments. Cyber is a constitutive element of our societies - its physical, economic, social, and political elements - and its security is essential to equitable and inclusive economic and social development and to the protection of human rights, yet while plenty of initiatives are available to industry, citizens are often left behind and ill-equipped to ensure their online safety. Because of its essential role, cybersecurity should be managed as a global public good.

This submission calls for a whole-of-society approach to addressing the cybersecurity needs of all segments of society and leverage existing best practices, efforts, tools, and solutions to respond and mitigate against growing cybersecurity threats.

Core principle that all governments, civil society organizations, and other stakeholders should adhere to:

Equip all segments of society with skills and affordable, action-oriented, easy-to-follow steps and easy-to-implement solutions to stay safe online.

Key commitments to bring about these specific principles.

Fund cybersecurity education programmes in schools and at the community level

The young generation, despite being digital natives, does not follow cybersecurity best practices. This trend is likely to continue unless cybersecurity training begins at an early age. Cybersecurity should be a part of the regular school curriculum and supported by public-private partnerships as the private sector has a responsibility to ensure that its future customers can use its products and services safely.

Promote cyber tools for all Internet users.

Ensure that citizens and businesses, whatever their situation and sector of activity, are not only aware of cybersecurity best practices, but have access to solutions and actually adopt and implement them. To do so, solutions need to be relevant, localized, affordable, and easily accessible. Governments and non-profits offer useful toolkits around the world. Support these stakeholders, promote existing initiatives, and encourage cooperation.

What our coalition has already committed to do

In April 2022, Craig Newmark Philanthropies announced a commitment of more than $ 50 million to support a broad coalition of organizations dedicated to a *Cyber Civil Defense* initiative. That coalition of entities is calling for a whole-of-society response to the escalating volume and sophistication of cyber-attacks.

There is consensus that a whole-of-society effort is required to address the challenges that cyber insecurity poses to economic development and equity. Cybersecurity needs to be inclusive. Different groups face different issues and have specific needs and requirements with respect to cybersecurity. In a whole-of-society approach, we must ensure that all needs, including those of underserved communities around the world, are represented and addressed.

Education and Skills

There's no denying the world is facing a cybersecurity skills gap. The coalition is committed to provide skills building for those who are not able to participate in certification programs and focus on the "skills to build", in addition to the current "certification to get" approach. More efforts should be dedicated to the mutual recognition of skills. Without that, cross-border cooperation and mobility remain challenging.

Tools and Services

In the whole-of-society, not every entity has the tools and services it needs to fulfil its responsibilities. The coalition committed to ensure that solutions are available and work at a global scale. The Global Cyber Alliance is launching a cybersecurity taxonomy project framed as a community-based initiative to identify all cybersecurity risks in the Internet infrastructure and at the end user level. The project aims to identify all current tools and solutions that address known cyber risks and provide the basis for community collaboration to identify gaps. The project will drive community collaboration and concerted action to develop tools and solutions that address those gaps and enable communities to protect themselves from cyber-risks.

Awareness

Building a community and working together to solve cyber insecurity is one aspect. The Global Cyber Alliance is committed to do everything possible to ensure awareness and usability of solutions, tools, and services, and meet the audiences where they are, and not expect greater expertise or commitment of resources than can reasonably be required in today's difficult environment.

Resourcing

The fight against cybercrime has so far received more resources than preventive cybersecurity and resilience. The focus of funding, whether from governments, the philanthropic community, or private sector investments, will determine whether tools and solutions for infrastructure operators and all user communities, including the most vulnerable, can be made available and accessible. Non-profit organizations, even those that provide essential services for the operation of the Internet, find obtaining resources for operations quite challenging. The coalition committed to call for a sustainable funding plan for cybersecurity, one that federates the necessary resources from funding to tools and human expertise to enable people - all people - to be protected.