Ethics Code of Conduct for Cyber Peace and Security (ECCC)

Version 3.0

Governor Michael Dukakis, Mr. Nguyen Anh Tuan, Mr. Allan Cytryn, Prof. Nazli Choucri, Prof. Thomas Patterson, Prof. Derek Reveron, Prof. John E. Savage, Prof. John Quelch, Prof. Carlos Torres.

The Boston Global Forum's Ethics Code of Conduct for Cyber Peace and Security (ECCC) makes the following recommendations for maintaining the security, stability and integrity of cyberspace.

Net Citizens Should

- Engage in responsible behavior on the Internet, e.g.
  - Conduct oneself online with the same thoughtfulness, consideration and respect for others that you expect from them, both online and offline
  - Do not visit suspicious websites
  - Do not share news or content from sources that are not trustworthy

- Learn and apply security best practices, e.g.
  - Update software when notified by vendors.
  - Ensure your PC has virus protection software installed and running.
  - Use strong passwords, change them periodically, and do not share them.
  - Do not transmit personally identifiable information to unknown sites.
  - Maintain a healthy suspicion of email from unknown sources.
  - For web communication use HTTPS instead of HTTP when possible.

Policy Makers Should

- Endorse and implement recommendations made by the 2015 UN Group of Governmental Experts (GGE), the Group of Seven (G7) and the Group of Twenty

Tel: +

(G20). Below we summarize the important norms concerning information and communication technologies (ICTs).

1. [GGE] International law, including the UN Charter, applies online.
2. [GGE] States should help limit harmful uses of ICTs, especially those that threaten international peace and security.
3. [GGE] States should recognize that good attribution in cyberspace is difficult to obtain, which means miscalculation in response to cyber incidents is possible.
4. [GGE] States should not knowingly allow their territory to be used for malicious ICT activity.
5. [GGE] States should assist other states victimized by an ICT attack.
6. [GGE] States, in managing ICT activities, should respect the Human Rights Council and UN General Assembly resolutions on privacy and freedom of expression.
7. [GGE] States should protect their critical infrastructure from ICT threats.
8. [GGE] A state should not conduct or permit ICT use that damages the critical infrastructure of another state or impairs its operations.
9. [GGE] States should work to ensure the integrity of the supply chain so as to maintain confidence in the security of ICT products.
10. [GGE] States should prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions.
11. [GGE] States should encourage reporting of ICT vulnerabilities and the sharing of remedies for them.
12. [GGE] States should not knowingly attempt to harm the operations of a computer emergency response team. Nor should it use such a team for malicious international activity.
13. [G7] No state should conduct or support ICT-enabled theft of intellectual property, trade secrets or other confidential business information for commercial gain.
14. [G7] If ICT activity amounts to the use of force (an armed attack), states can invoke Article 51 of the UN Charter in response.
15. [G7] States should collaborate on research and development on security, privacy and resilience.
16. [G7] States are encouraged to join the Budapest Convention.

- States should not create nor tolerate the dissemination of fake news.

IT Engineers Should

- Apply best practices in the design, implementation and testing of hardware and software products so as to
    - Avoid ICT vulnerabilities,
    - Protect user privacy and data
- Make use of the NIST "Framework for Improving Critical Infrastructure Cybersecurity" as a guide for improving the security of critical applications.
- Should not create nor use technology to create or disseminate fake news.

Business Firms and Business Leaders Should

- Take responsibility for handling sensitive corporate data stored electronically.
- Create employment criteria to ensure that employees are qualified to design and implement products and services that meet high security standards.
- Ensure that IT engineers are kept abreast of the latest ICT security threats.
- Implement effective Cyber Resilience in your business.
- Engage in information sharing of ICT hazards, subject to reasonable safeguards, with other companies in similar businesses.

Educators, Influencers/Institutions Should

- Teach the responsibilities of net citizens described above, including fostering good behavior and avoidance of malicious activity.
- Help global citizens to acquire the critical thinking skills needed to identify and avoid fake news and discourage its dissemination.
- Ensure that IT engineers are taught the skills necessary to produce safe, reliable and secure ICT products and services.
- Educate and lead global citizens to support and implement the ECCC.
- Create honors and awards to recognize outstanding individuals who contribute greatly to a secure and safe cyberspace.