

A Digital Geneva Convention to protect cyberspace

Microsoft Policy Papers



Advancing a Digital Geneva Convention to protect cyberspace in times of peace

Governments continue to invest in greater offensive capabilities in cyberspace, and nation-state attacks on civilians are on the rise. The world needs new international rules to protect the public from nation-state threats in cyberspace. In short, the world needs a Digital Geneva Convention.

Although no international agreement is ever perfect, the world has already benefited from other global covenants. The Treaty on the Non-Proliferation of Nuclear Weapons and the Chemical Weapons Convention are both examples of the international community coming together to effectively manage weapons with the potential to create catastrophic harm.

A Digital Geneva Convention would create a legally binding framework to govern states' behavior in cyberspace. While there is a need for urgency and even high ambition, steps can also be taken incrementally. There are important opportunities to progress towards a legally binding agreement through initial voluntary or politically binding efforts, such as those underway within the United Nations or the [Group of Twenty Countries \(G20\)](#)¹. Ultimately, whatever the route, arriving at a legally binding framework would establish new rules for governments and help protect cyberspace in both peacetime and prevent conflict.

We can build on existing proposals for responsible state behavior in cyberspace

The process of creating the Digital Geneva Convention involves formidable challenges. It will require political will and commitment from government leaders across the world. Some important foundations have already been put in place, however, and offer a starting point to create an effective international legal framework.

The [UN-Government Group of Experts](#)² proposed a new set of rules and principles for the responsible behavior of nation states in cyberspace in 2015. Adhering to these behaviors or "norms" is voluntary, but over time some experts believe that they could evolve into customary international law. In February 2017, the [Global Commission for the Stability of Cyberspace](#)³ was launched by the Dutch government, the Hague Center for Strategic Studies, and the East-West Institute to, "develop proposals for norms and policies to enhance international security and stability and guide responsible state and non-state behavior in cyberspace." In addition, a series of other expert groups and civil society organizations have contributed a range of well thought out ideas and proposals.

However more work remains to be done to advance transparency of, and accountability for, state behavior in cyberspace. A pragmatic and flexible path to get deliver that vision should be identified. This should become an urgent priority for the world's leading cyber powers.

¹ https://www.g20.org/Webs/G20/DE/Home/home_node.html

² <https://www.un.org/disarmament/topics/informationsecurity/>

³ <https://cyberstability.org/>



A Digital Geneva Convention to protect cyberspace

Microsoft Policy Papers



The substance of a Digital Geneva Convention for Peacetime

Governments have established and followed international rules in other military and geopolitical areas such as non-proliferation. Cyberspace should not be different. The key clauses at the center of the Digital Geneva Convention should commit states to:

- Refrain from attacking systems whose destruction would adversely impact the safety and security of private citizens (i.e., critical infrastructures, such as hospitals, electric companies).
- Refrain from attacking systems whose destruction could damage the global economy (e.g., integrity of financial transactions), or otherwise cause major global disruption (e.g., cloud-based services).
- Refrain from hacking personal accounts or private data held by journalists and private citizens involved in electoral processes.
- Refrain from using information and communications technology to steal the intellectual property of private companies, including trade secrets or other confidential business information, to provide competitive advantage to other companies or commercial sectors.
- Refrain from inserting or requiring “backdoors” in mass-market commercial technology products.
- Agree to a clear policy for acquiring, retaining, securing, using, and reporting of vulnerabilities – that reflects a strong mandate to report them to vendors – in mass market products and services.
- Exercise restraint in developing cyber weapons and ensure that any that are developed are limited, precise, and not reusable. States should also ensure that they maintain control of their weapons in a secure environment.
- Agree to limit proliferation of cyber weapons. Governments should not distribute, or permit others to distribute, cyber weapons and should use intelligence, law enforcement, and financial sanctions tools against those who do.
- Limit engagement in cyber offensive operations to avoid creating mass damage to civilian infrastructure or facilities.
- Assist private sector efforts to detect, contain, respond, and recover in the face of cyberattacks. In particular, enable the core capabilities or mechanisms required for response and recovery, including Computer Emergency Response Teams (CERTs). Intervening in private sector response and recovery would be akin to attacking medical personnel at military hospitals.

The pressing case for launching a dialogue

Effective cybersecurity is critical to international peace and economic stability. The Digital Geneva Convention can play the central role in safeguarding citizens around the world from state-led or state-sanctioned cyberattacks in times of peace. By building on the work done to date, governments, the technology sector and civil society groups can pave the way for a legally binding agreement that will ensure a stable and secure cyberspace. Everyone with an interest in advancing this process should commit to working with public sector and private sector partners around the world to find a practical way forward.

