2020 UN General Assembly

Connecting through Crisis

Digital Peace:

Trust & Security in Cyberspace

eurasiagroup Microsoft GZERO

Digital Peace: Trust & Security in Cyberspace

Three years ago, long before anyone had ever heard of Covid-19, a different kind of virus spread around the world: A piece of malicious software code launched by a nation state. It paralyzed computer networks in hundreds of countries, disrupted global shipping, forced pharmaceutical factories to shut down, and inflicted an estimated $10 billion of economic damage.

On the physical battlefield, a widely accepted set of rules, backed by international law, governs conduct, with the aim of protecting soldiers and civilians. Establishing common rules or guardrails is much harder in cyberspace, where borders can't be easily defined and the tools and tactics of combat are always changing. But it has never been more urgent.

Against this chaotic cyber backdrop, how can governments protect critical healthcare infrastructure and medical research as they mobilize in response to Covid-19? How can citizens and companies work together to prevent the smart phones and computers they rely on for work, education, and staying connected from being hijacked and used to carry out malicious cyberattacks?

The UN has been working for over a decade to establish basic principles, or "norms" in the parlance of international diplomacy, for cybersecurity. But this problem can't be solved by any one government or group of governments on their own. In recent years, as threats have multiplied, global companies, cybersecurity researchers, and non-governmental organizations have taken a seat at the table. Establishing norms and boundaries around acceptable behavior doesn't mean just modernizing the existing architecture of international governance. It involves re-thinking it to account for a 21st century in which life, business, and diplomacy are digitized and the lines between them increasingly blurred.

What's the UN doing about it?

The United Nations has been facilitating discussions on cyber norms since 2004. Discussions at the UN are currently following two tracks. One track, known as the Group of Governmental Experts, consists of representatives from 25 member states. This group has a mandate to study norms, rules and principles of responsible behavior for states in the cyber realm; and to undertake confidence-building and capacity-building measures. Another track, known as the Open-Ended Working Group, is open to any UN member state, as well as the business community, academia, and civil society. This group is expected to issue a report to the General Assembly this month.

How are others trying to help?

In recent years, businesses and non-governmental organizations have intensified their efforts to raise awareness, analyze cyberattacks, develop norms, share best practices, and increase pressure on governments to act. Governments are critical players by deciding how and when to use state cyber capabilities, but the private sector bears actual responsibility for securing and defending the networks that people rely on for their livelihoods and essential services.

In May, the CyberPeace Institute, an independent initiative dedicated to enhancing the stability of cyberspace, backed by Microsoft, Mastercard, the William and Flora Hewlett Foundation, and other corporate and non-profit sponsors, called on world governments to take "immediate and decisive action" to stop cyberattacks against hospitals, medical research facilities, and international public health organizations.

What's needed next?

To achieve lasting stability in cyberspace, governments must decide that it's in their own interest to accept limits on how they deploy offensive cyber capabilities in pursuit of political and strategic goals. To achieve this, governments, international organizations, companies, NGOs, and ordinary citizens all will have to work together to raise awareness of the risks that malicious exploitation of the internet poses for people's lives and livelihoods.

This is a complex challenge that can't be solved by any one group acting alone. International dialogue is just the first step. Eventually, widely agreed norms have the potential to evolve into laws and treaties, but before that can happen, all of the groups with a stake in the outcome need to:

1. **Build confidence:** The lack of trust between governments, and between governments and industry, is a big barrier to cooperation. Exchanging information, including establishing hotlines between governments, is one way to build trust.
2. **Build capacity:** Companies and governments that have already implemented tough cybersecurity measures can improve security for everyone by sharing best practices. Countries can also work together, including through international venues such as the UN, to strengthen their capacity to conduct cyber diplomacy.

How can I get involved?

Cybersecurity is a rare field of international diplomacy in which ordinary citizens can make a real difference. It starts with protecting yourself, your family, and your workplace from common cyber threats. Easy-to-use security features like strong passwords, virtual private networks, and two-factor authentication, which requires a user to enter a code or use a hardware fob in addition to their password when logging in, can help protect sensitive accounts and data. Learning about how hackers can try to manipulate people into voluntarily giving up their passwords or downloading malicious code onto their computers via deceptive emails or phone calls can improve not just your personal security, but the resilience of the entire internet against cyber threats.