CYBER PEACE & SECURITY MONITOR

Civil society perspectives on the Open-ended working group on developments in the field of information and telecommunications in the context of international security

VOL.01 NO.01

9 September 2019

Photo: Philipp Katzenberger

IN THIS ISSUE

Reaching Critical Will

www.reachingcriticalwill.org

A PROGRAMME OF THE WOMEN'S INTERNATIONAL LEAGUE FOR PEACE & FREEDOM

www.wilpf.org

OPPORTUNITY AND IMPERATIVE—CAN A NEW UN WORKING GROUP ON CYBER SECURITY BRING SECURITY FOR ALL?

Allison Pytlak | Reaching Critical Will, Women's International League for Peace and Freedom

It's always exciting when a new UN process gets underway and there is the potential to break free of entrenched dynamics or tackle new challenges. The Open-ended Working Group (OEWG) on developments in the field of information and telecommunications in the context of international security represents just such an opportunity. But we will need to guard against falling into the political gridlock of prior discussions on this subject while protecting the gains already made. We also need to seize this opportunity to prevent the growing militarisation of cyber space and orient towards cyber peace based on human rights and equity.

An omnipresent threat

It's hard to imagine another topic as ubiquitous as information and communications technologies, or ICTs. ICTs are integrated into nearly every facet of our lives in some way or another. That is what makes their vulnerability—and relatedly, our vulnerability—to attack or misuse so great.

We now use the term "cyber security" in reference to an ever-widening spectrum of activities guarding against espionage, surveillance, privacy intrusions, denial-of-service attacks, ransomware, and malware operations that variously impact countries and individuals. Many of these activities have the ability to disrupt, disable, or destroy vital physical infrastructure or national or human security. Some constitute criminal activities, while others occur within legal grey areas. Cyber operations have become an effective tool to sow disruption or confusion and are transforming espionage. Moreover, digital technology has added new means by which governments can control or repress the human rights of their citizens.

There are also important points of intersection with militarism and traditional arms proliferation: for example, the dark web facilitates illicit arms trafficking. Surveillance technologies pose risks to privacy and can also be used to target strikes with armed drones and other weapons. The vulnerability of certain weapon systems—notably nuclear weapons, uncrewed aerial vehicles (drones), and potentially autonomous weapons, if developed—to digital attack present new areas of alarm, but also compelling incentives to eliminate those weapons.

Yet, at least in the context of the United Nations, states have struggled to come up with the types of policy and legal responses that reflect the urgency of these threats, which has prompted action in other forums. This subject has been officially on the UN's agenda since 1998 and Groups of Governmental Experts (GGEs) on ICTs have been meeting since 2004. The GGEs have produced results in the form of agreement over the applicability of international law to cyber space and actions therein, as well as articulating recommendations for norms, rules, and principles for state behaviour and reinforcing respect for human rights and fundamental freedoms. Yet they also met without any transparency, in closed and unrecorded sessions, and were limited in number. Over time, fundamental differences in approach and perspective prevented further progress within the GGEs, while at the same time more member states, alongside other actors, began to call for greater openness and claim their role as rightful stakeholders in this conversation. As the OEWG begins its work, it will need to account for a parallel discussion in a new (2019-2021) GGE; the outcomes of external, non-UN processes; and the rapid pace of technological development.

Can we escape geopolitical realities? Should we?

The OEWG's establishment occurred in a context of intense politicisation that characterised the 2018 First Committee. Souring US-Russia relations, especially in relation to nuclear disarmament and non-proliferation, coupled with growing animosity between the US and Iran, and ongoing disputes over attribution for chemical weapons use in Syria, coloured the entire 2018 session and was undoubtedly a contributing factor to the establishment of two concurrent UN processes

devoted to cyber security.

These realities have not disappeared and if anything, have only deepened. At the same time, real world cyber operations are increasing, with a constant stream of revelations that include electoral disruption, power grid attacks, or database meddling—not to mention truly terrifying information about how governments use ICTs to spy on, harass, harm, and control populations. Some of the governments most implicated in these activities are the same as those who have found themselves at odds in past GGEs.

Discussions in the First Committee and its mandated bodies have at times occurred in a deliberate vacuum, which can make dialogue easier, but in turn, may reduce the impact of decisions made. It is difficult to know if or how states will choose to bring these realities into Conference Room 4 and what influence that could have. Overcoming antagonism between the states that are most frequently responsible for hostile cyber operations—yet who also view themselves as the among the entrepreneurs of cyber norms—will be key to breaking stalemate and arriving at solutions that work for all states. It is also another reason why it's time for a larger number of governments and other actors to have a voice in this arena.

Broadening the discussion?

When the vote was taken in November 2018 on the resolution that established the OEWG, the Russian Federation as its main sponsor explained at length how this format will bring the inclusivity and openness that the wider UN membership has been seeking on this issue. Not only are all meetings open to all member states, rather than a select few, but the resolution also provides for a two-day consultation with civil society and private industry, scheduled now for December 2019. At the time, this speech was interpreted by many as a dig at the US-sponsored resolution proposing another closed GGE—albeit one with new input mechanisms—while appealing to the growing calls for more open, inclusive, and transparent discussions on this subject that had been voiced in earlier First Committee sessions.

Yet, despite the grandstanding, doors are already being closed. Certain (unnamed) member states have objected to the participation in the September session of the OEWG of any non-governmental organisation that does not have ECOSOC status. This has affected a total of 18 organisations that had sought accreditation to this session, and includes well-known think tanks, research institutes, advocacy networks, and private technology companies that together possess significant knowledge and expertise in this area. Such a broad and categorical denial of access is extremely rare in UN disarmament and arms control fora and sets a dangerous precedent.

Having more voices at the table in the form of the full UN membership should inevitably open up the conversation to new priorities and perspectives from a broader cross-section of countries than those who were able to participate in the earlier GGEs. It could also help to dilute and diffuse some of the tensions described above. This is of course, if the OEWG can escape the same power dynamics that have come to characterise so many other UN security bodies, in which the voices of a global majority are stifled by a powerful few. To achieve this, wider civil society participation is an imperative, not a threat.

Having more voices at the table should inevitably open up the conversation to new priorities and perspectives.

Concerns about restricted access aside, the format of this first session sends a positive signal. It will allow for an airing of views via a general exchange, as well as providing time for thematic debate on the six areas highlighted in resolution 73/27: existing and potential threats; international law; rules, norms and principles; institutional dialogue; confidence building measures; and capacity-building.

For many states, it will be the first time that their views are heard on this subject and can devote greater time and depth to each of these aspects than a normal First Committee statement would

allow for. States are encouraged to come prepared to share existing policy and practice, and their priorities. States should also be encouraged to use this week, and further OEWG sessions, to delve beyond topline messaging and rhetoric and bring greater specificity into the discussion around threats and present the ways in which they are already working together to build confidence, share information, and build capacity. This will enable a better mapping of the current landscape and identify where gaps and differences remain, in order to direct forward work and assess progress against already agreed norms and principles.

A question of mandate

Something that certain civil society watchers are curious about is where the conversation across these six topics will go and how closely they will remain within the "context of international security," as stated in the name of OEWG. What this means in UN-speak is, will they remain within the bounds of national-security first approaches?

This is not to say that national security is not important, but that frequently this approach prioritises military interests and superiority over the security and well-being of people. To date, discussions about cyber security in the First Committee have had a sanitised and somewhat abstract tone that has broadly overlooked the human impact of malicious cyber operations, whether carried out between governments or by governments toward their own populations. There are countless references to "critical infrastructure" but far fewer to protecting people or at least, linking up in a meaningful way how an attack on infrastructure further renders harm to citizens and civilians. There are also awkward and somewhat square-peg-in-round-hole efforts to graft military concepts and disarmament language or approaches onto cyber security discussions. So-called "cyber weapons" will never be tangible in the same way that missiles or guns are and talking about deterrence in a context where attribution is challenging at best and impossible at worst is a poor fit. The slow creep of this language into this landscape demonstrates, and simultaneously reinforces, the extent to which we are collectively allowing cyber space to become militarised. It implies a tacit acceptance of the weaponisation of technology in which our starting point for policy and legal response takes this as a baseline and not as something to oppose and prevent. For WILPF, the militarisation of cyber space represents an expansion of the patriarchal structures of power that perpetuate violence and repression in the offline world. It is an approach that not only overlooks systemic and root causes of violence but sets out to exacerbate or create violence in a new medium where it does not necessarily otherwise occur.

To date, discussions about cyber seucurity in the First Committee have had a sanitised and somehwat abstract tone that has broadly overlooked the human impact of malicious cyber operations, whether carried out between governments or on their own populations.

Some states, and a few NGOs, are skittish about bringing these perspectives to the table, particularly where it intersects with human rights concerns. This is for a diversity of reasons, including a preference for UN siloes, varying understandings of what security means, but also for potentially losing gains made in other spaces, notably around digital human rights protection.

Yet even when official siloes are maintained we have seen before that it is very possible to approach a security issue with a human lens and humanitarian approach. The Treaty on the Prohibition of Nuclear Weapons, which emerged from a UN General Assembly (UNGA) process, has enshrined in law global recognition and desire to prevent the catastrophic humanitarian consequences of nuclear weapons and transformed the discourse on how we talk about nuclear arms. The Arms Trade Treaty, which also emerged from the UNGA, has human rights

and humanitarian impact at its core. The current surge of support for addressing the gendered impact of armed violence and conflict within the disarmament community embodies this approach and could likewise be applied to the digital landscape where online forms of gender-based violence are just as egregious as what takes places offline.

Moreover, a very genuine crossover exists in the area of cyber security given the extent to which digital technology touches all our lives. Some international or inter-state cyber operations undermine democratic institutions and risk escalating a situation into conflict, and there is the possibility that decisions taken in the pursuit of cyber stability could adversely affect human rights by promoting measures of state control over information.

For this reason, we encourage states participating in the OEWG to come ready to expand the discourse in ways that recognises the negative repercussions of hostile cyber operations on people and stop treating this as a secondary after-thought. It's time to use the opportunity of a new format and fresh start to deliver on a form of cyber security that actually makes us safer.

WILPF is providing coverage and analysis of the OEWG session.

Visit www.reachingcriticalwill.org

for conference documents, statements, links to other resources and future coverage.

CYBER PEACE & SECURITY MONITOR

Reaching Critical Will is the disarmament programme of the Women's International League for Peace and Freedom (WILPF), the oldest women's peace organisation in the world. Reaching Critical Will works for disarmament and the prohibition of many different weapon systems; confronting militarism and military spending; and exposing gendered aspects of the impact of weapons and disarmament processes with a feminist lens. Reaching Critical Will also monitors and analyses international disarmament processes, providing primary resources, reporting, and civil society coordination at various UN-related forums.

Reaching Critical Will

www.reachingcriticalwill.org

www.wilpf.org

The Cyber Peace & Security Monitor is produced by the Reaching Critical Will programme of the Women's International League for Peace and Freedom (WILPF) during relevant UN meetings.

CYBER PEACE & SECURITY MONITOR

Vol. 01, No. 01
9 September 2019

Editor: Allison Pytlak
disarm@wilpf.org