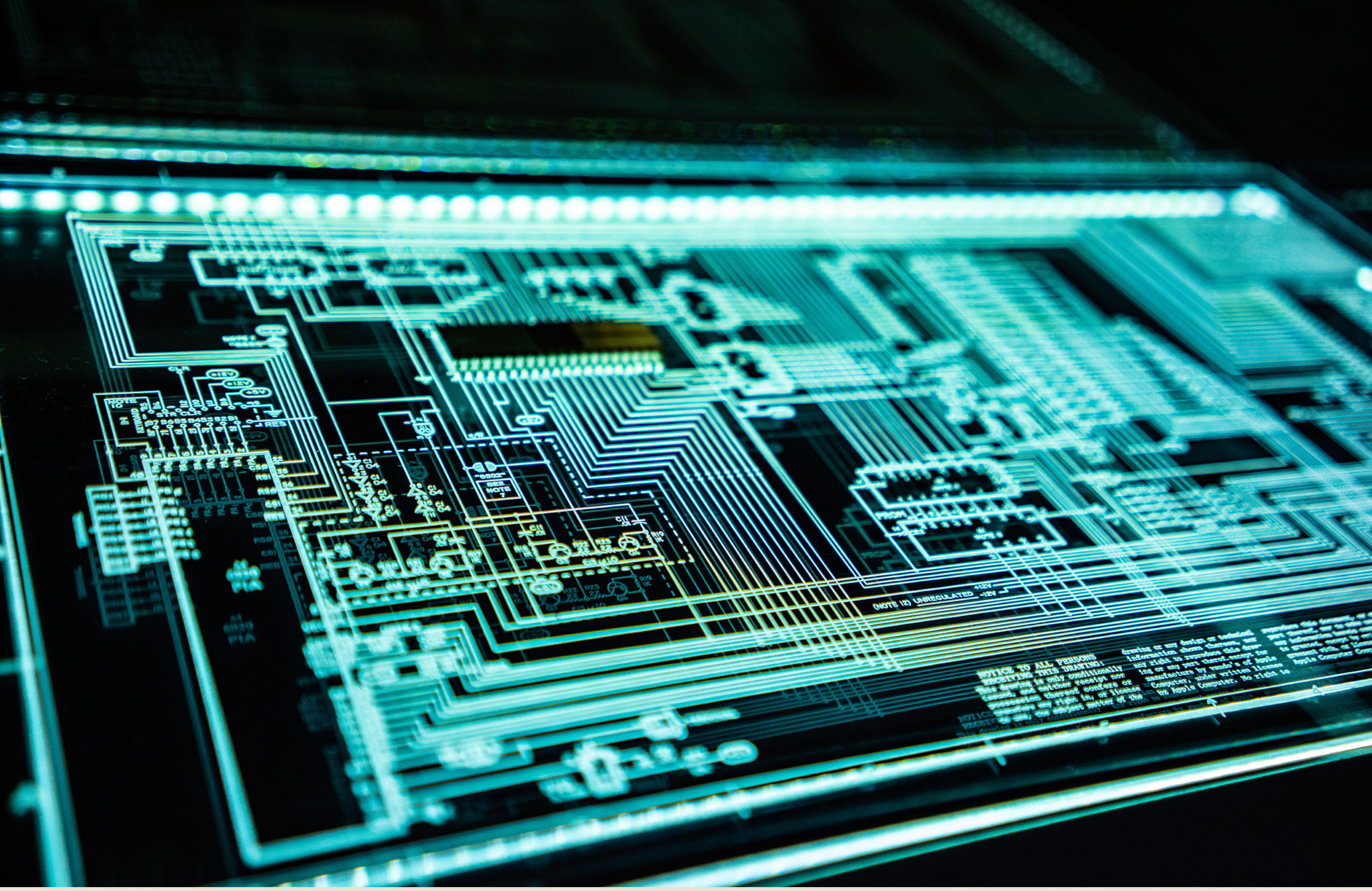

PROGRAMMING ACTION:
OBSERVATIONS FROM SMALL ARMS CONTROL FOR CYBER PEACE

WOMEN'S INTERNATIONAL LEAGUE FOR
PEACE & FREEDOM

FEBRUARY 2021
PROGRAMMING ACTION: OBSERVATIONS FROM SMALL ARMS CONTROL FOR CYBER PEACE
1st edition
19 pp.

Written by Allison Pytlak

Edited by Ray Acheson, with inputs and review from Joseph Dube, Ed Laurance, Daniel Mack, and Paul Meyer.

Cover photo: Adi Goldstein / Unsplash

TABLE OF CONTENTS

Introduction

Malicious international cyber operations have become one of the most pressing security issues of our time. States and non-state actors still wage war with physical weapons, but they are increasingly turning to "attacks" and operations that employ information and communications technologies (ICTs) to provoke their opponents, or that transform digital networks into mediums for aggression or disruption. The scale and severity of these operations is rising, especially during the COVID-19 pandemic.

This has prompted some governments to call for an international treaty to regulate state behaviour in cyber space. Others maintain that the existing patchwork of voluntary norms is sufficient—but that these norms require more effective implementation or monitoring to be effective. A potential compromise has emerged in a proposal for a programme of action (PoA) on cyber security and state behaviour in cyber space. This has been suggested in the context of the UN's Open-ended Working Group (OEWG) on developments in the field of information and telecommunications in the context of international security.

Political appetite for such an instrument is growing. Yet, questions remain: what commitments would such a future instrument include? What kind of accountability and monitoring mechanisms could it establish? What does "politically binding" mean? What is the role of non-governmental stakeholders?

Some states have suggested modelling a cyber PoA on the United Nations Programme of Action to Prevent, Combat and Eradicate the Illicit Trade in Small Arms and Light Weapons in All Its Aspects (UNPoA). This instrument was considered a breakthrough achievement when it was adopted in 2001. It was the outcome of focused collaboration between like-minded governments and civil society who shared the goal of stopping the uncontrolled proliferation of small arms and light weapons (SALW) in order to save lives and reduce human suffering.

The Women's International League for Peace and Freedom (WILPF) has, through its disarmament programme Reaching Critical Will (RCW), followed the UNPoA on small arms for nearly two decades. National WILPF sections have conducted advocacy and supported governments to meet their UNPoA commitments, while its international staff have monitored all UNPoA meetings held at the UN since 2008, through its Small Arms Monitor. WILPF is a member of the International Action Network on Small Arms (IANSA), the global civil society network that gave rise to the small arms UNPoA and works for its implementation.

In recent years, WILPF has expanded its disarmament and security work to include information and communications technologies (ICTs) and cyber peace, by monitoring and reporting on relevant UN fora[1] as well as conducting research on the gender dimensions of international cyber security[2] and challenging the militarisation of cyberspace.[3]

It is from this perspective that WILPF offers this briefing paper as food for thought to both states and stakeholders interested in advancing a cyber PoA. We have identified five observations from our experience in engaging with the small arms UNPoA that we deem relevant for the international cyber security community to consider as it moves forward. This briefing paper is informed by interviews with other civil society experts, as well as publicly available analysis and commentary.[4] It does not at this stage set out our views on what a cyber PoA should include as content, but does offer some broad recommendations in relation to substance as well as procedure.

For clarity, the author uses "UNPoA" to refer to the programme of action on SALW because it is an established instrument adopted under the auspices of the United Nations, and "cyber PoA" for a possible future cyber programme of action.

The state of play on a cyber programme of action

In October 2020, a cross-regional group of member states led by Egypt and France put forward a proposal in the context of the UN's cyber OEWG. The document suggested that the OEWG could "explore establishment of a Programme of Action for advancing responsible State behaviour in cyberspace with a view to ending the dual track discussions (GGE/OEWG) and establishing a permanent UN forum to consider the use of ICTs by States in the context of international security."[5]

The proposal for a PoA on "responsible state behaviour in cyberspace" would, per the document submitted to the OEWG, provide states with the opportunity to create a framework and a political commitment based on recommendations, norms, and principles already agreed; have regular, working-level meetings focused on implementation; step up cooperation and capacity-building; have regular review conferences to ensure the PoA is adapted and updated; and organise consultations with other stakeholders and relevant multi-stakeholder initiatives.[6]

During the UNGA First Committee session in October–November 2020, several states spoke favourably of the proposal with some noting that it would be a bridge between calls for a legally binding instrument (a treaty) and the current voluntary normative framework.[7]

A larger number of states submitted an updated proposal in December 2020 around the time of the OEWG's informal consultations on the subject of "regular institutional dialogue".[9] The higher number of states listing as submitting the proposal reflects a growing number of formal supporters. A fuller concept note was also shared with member states and published to the OEWG website in December. The concept note covers wide ground, including both procedural and substantive ideas. There are proposals for the frequency of its meeting cycle, decision-making procedures at those meetings, and participation for non-governmental stakeholders.

Substantively, the authors of the concept note suggest that the actual instrument take the form of a "politically binding declaration" that would be based on the reports of the UN's Group of Governmental Experts (GGE) on responsible state behaviour in cyberspace that were issued in 2010, 2013, and 2015, as well as the expected reports of the current OEWG and the current GGE, which will both complete work in 2021. The concept notes that "Consensus principles, recommendations and commitments could be added to that declaration, in order for the PoA declaration to be a standalone establishing document. The political declaration and subsequent implementation action should address International Law, Norms, Rules and Principles, CBMs and Capacity Building." There is also the suggestion that states begin to submit voluntary national reports on their implementation of the cyber PoA, which builds from proposals made earlier to the OEWG.

One path forward for a cyber PoA would be to see its creation recommended within the final report of the OEWG, and potentially the GGE's as well. States supportive of a cyber PoA have tabled draft text[9] for possible inclusion in the OEWG final report—the "zero draft" of which was released in mid-January 2020,[10] and does recommend a cyber PoA. The OEWG's third substantive session is currently scheduled for March 2021, at which time it is expected to agree and adopt an outcome report.

Later in 2021, a second OEWG will begin work to follow on from the first. It will be open until 2025. The GGE is also slated to conclude its work in 2021.

With a recommendation from the OEWG and/or the GGE, states would have firm footing to introduce a resolution at the UNGA First Committee in October 2021 calling for a negotiating conference, likely in 2022.

At the time of writing, it's difficult to assess with certainty where this proposal will go. Around one-quarter of UN member states have formally supported the PoA suggestion,[11] with others indicating strong interest or informal support. At the time of writing, there is not any significant, formal opposition—although certainly many states have questions about this proposal or have not expressed a position yet. Civil society did not have access to the informal OEWG consultations in December where this was addressed, so it's not possible to know if any significant opposition has been expressed there. During the 2020 UNGA First Committee session, most references to a cyber PoA were positive.[12]

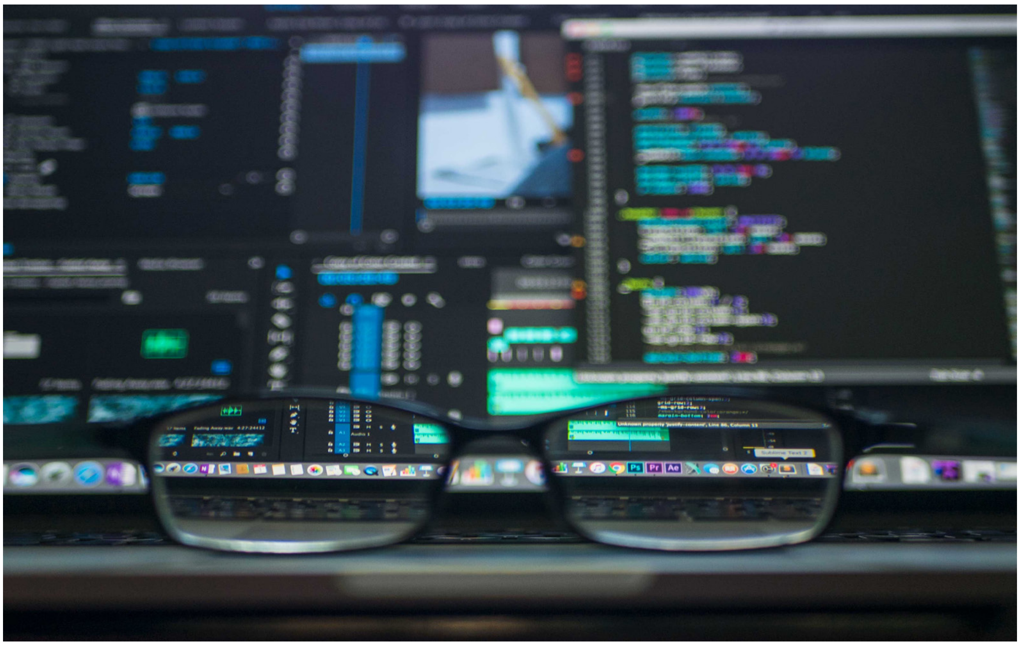

Photo: Kevin Ku / Unsplash

Overview of the UNPoA on small arms and light weapons

What is it?

A programme of action can perhaps best be explained as exactly that: an outline, or programme, of practical actions that endorsing parties agree to implement as a way to achieve stated shared objectives. Programmes of action focus on behaviour and activities. A programme of action constitutes a standalone instrument that, while not legally binding in the way that a treaty is, does signal commitment to implement the practical actions contained therein.

Programmes of action go beyond political declarations in their level of detail and specificity. They also often include more provisions for monitoring and follow-up than declarations. But both types of instruments are similarly endorsed at a political level (often high-level) and do not require national legislative review. They are viewed as a good compromise when a legal instrument is not politically feasible or viable. Programmes of action are negotiated instruments or documents. When they are to be the product of a UN process, they require an initial mandate from UN member states to commence negotiations.

The UNPoA on SALW has four sections.[13] The **preamble** situates the instrument in a context of other relevant instruments, UN resolutions, and decisions. Importantly, it also outlines clearly the humanitarian concerns and objectives that underpin the agreement and the resolution of those adopting the instrument to "prevent, combat and eradicate the illicit trade in small arms and light weapons in all its aspects". This includes in relation to poverty, conflict, socioeconomic development, negative impacts on women, human dignity, and child rights, amongst others.[14]

Section II, "Preventing, combating and eradicating the illicit trade in small arms and light weapons in all its aspects," is the substantive heart of the instrument. This section outlines the specific actions that states agree to undertake in order to meet the objectives set out in the preamble. These actions are detailed in 40 paragraphs that are organised at national, regional, and global levels and include activities that cover, for example, collecting and destroying illegal weapons; strengthening import and export controls; and improving the security and safety of weapons storage facilities. The sub-section on global actions makes references to the submission of voluntary national reports on UNPoA implementation.

Section III, "Implementation, international cooperation and assistance," recognises that to address the illicit trade in SALW, states cannot work in isolation—although they do bear primary responsibility for meeting their UNPoA commitments. This section includes actions that states should, or would be encouraged to, undertake to foster cooperation among each other and with other relevant stakeholders such as regional organisations and civil society.

Section IV outlines measures that are a follow-up to the 2001 conference where the UNPoA was adopted. This includes having a first review conference and biennial meetings of states, as well as requesting a UN study and encouraging cooperation and resource mobilisation to support implementation of the instrument.

Like most other products of consensus-driven processes, the final instrument reflects compromises and does not include the full range of commitments that some early proponents would have wanted it to. There are many qualifiers in the text (i.e. "when possible" "as appropriate"). In some instances, this has led to the creation of other, related, frameworks that attempt to fill those gaps, as will be discussed later. Other issues have continued to be sources of political discord and division during international UNPoA meetings.

How was it established?

The small arms UNPoA did not emerge overnight. It grew out of years of joint civil society and governmental advocacy and awareness-raising to put the issue on the UN's agenda, premised on a tragically ever-growing evidence base detailing the negative real-world consequences and harms caused by unchecked small arms proliferation in diverse countries around the globe. Coming on the heels of the successful negotiation of the Ottawa Convention banning anti-personnel landmines in 1997, the UNPoA emerged in an environment of heightened global cooperation and mobilisation between governments and civil society to advance people-first approaches to disarmament and arms control.[16]

The official timeline includes a series of movements within the UN setting, beginning with the establishment of a UN Panel of Governmental Experts on Small Arms by the UN General Assembly (UNGA).[17] Based on inputs received during regional workshops as well as its own sessions, the Panel produced two reports, in 1997[18] and 1999,[19] for the UN Secretary-General (UNSG). The reports outlined the scale and scope of the problem, as well as summarised relevant UN initiatives to address small arms such as UN Security Council decisions pertaining to specific conflicts in which small arms were a factor, or the pending negotiation of the Firearms Protocol as supplement of the UN Convention against Transnational Organized Crime. The reports also surveyed national and regional measures, including if and how the recommendations of the 1997 report were being addressed.

The 1999 report acknowledged that the UNGA had, in 1998, adopted a resolution[20] calling for the UN "to convene an international conference on the illicit arms trade in all its aspects no later than 2001."

That conference took place in July 2001 and its primary purpose "was to consolidate and coordinate small arms initiatives and develop an action agenda."[21]

While the conference was contentious, states were able to come to agreement on multiple points, which together formed the instrument that was adopted at the end of the conference as part of the final conference report. This was done without a vote. It's important to note that agreement was facilitated by the convening of three preparatory committees (PrepComs) in advance of the July conference. In addition, earlier regional initiatives and commitments on small arms had already developed standards and norms to use as a basis for the development of the UNPoA, as will be discussed later. Civil society played a central role throughout the process, as will be described in more detail later in this paper.[22]

Five observations from the small arms UNPoA process

The UNPoA on small arms is not the only UN programme of action, but it is the only one that has emerged from the UN General Assembly's First Committee on Disarmament and International Security, which is where the cyber OEWG also has its roots. The two issues of cyber security and SALW proliferation have some important differences that cannot be overlooked—yet given the similarities in the UN political climate around security and disarmament issues writ large, there are some key observations and lessons that can be applied.

Observation 1: Achieve clarity on the instrument's goals and scope early on.

Programmes of action are motivated by the shared goals of endorsing states and supportive stakeholders. These goals and purposes should serve to underpin the diverse substantive actions contained in the instrument—and provide the ultimate yardstick by which successful implementation will be measured.

The small arms UNPoA was bred out of a strong collective desire to alleviate the human cost of illicit SALW proliferation. These impacts were outlined strongly in the UN Panel of Experts' reports, as well as in countless other reports and testimonies provided by diverse civil society organisations. Several governments came forward around this time to champion the issue by hosting thematic conferences on SALW control, while also engaging with civil society in the areas of brainstorming for policy initiatives, holding consciousness-raising seminars, and funding programs to assist reintegration of former combatants and to collect and destroy weapons.[23] Others were also developing regional initiatives, to be discussed in the next sub-section. The three PrepComs held in advance of negotiations enabled a necessary space to exchange views, understand differences in position, and begin to identify points of commonality.

Yet for all the good will and positive momentum, once the moment arrived in July 2001 to actually develop the instrument, differences arose that spoke to the complexity of the issue and how to best situate the solutions that the PoA would include under common goals and framing: is it a problem of illegal arms supplies, beyond state control? Is it an issue of diverted legal transfers? Is it a crime problem? A socioeconomic development problem? All of the above? In short: what difference should this new instrument seek to make?

Different views about the instrument's purpose also illustrated various political motivations and pressures depending on if, for example, a state was an arms producer, or an importer; the extent to which it is affected by armed violence and conflict, etc. These roles had implications for where the burden of national UNPoA implementation would fall heaviest. In connection with these conflicting visions and priorities, the 2001 conference was tense and contentious at times. One state announced its "redlines" at the opening of the conference in such hostile tones that it not only came as a surprise to other states but also alienated them and changed dramatically what was open for negotiation at the conference.[25] Differences existed around very specific issues, in particular in relation to "limiting arms to nonstate actors, norms and standards on civilian possession of weapons, restrictions on the legal trade and manufacture of small arms, and follow-up processes aimed at negotiating legally binding treaties. When the PoA was finalized, all references to nonstate actors, civilian possession, and legally binding treaties had been removed."[26]

As one civil society small arms expert noted in an interview for this briefing paper, "The original ideas [for the PoA] had to do with revolutionising how countries and societies dealt with small arms in virtually every aspect that can be imagined. The original thrust was much more ambitious than what we got—it was reeled back 20-fold."

International cyber security is likewise complex and multi-faceted. The "solutions" or actions that a cyber PoA could include are manifold—and it's not yet clear precisely what glue will bind them together, or how wide-ranging the agreement will be.

States will come to negotiations from different levels of technological development, and varying experience in participating in other cyber security forums. Each will have its own understanding of the threat landscape and national priorities. This will influence what each believes the goals and objectives of the PoA should be—which, in turn, will impact what action points and substance that it eventually includes, and instrument's strength and ability to have real impact.

Therefore, developing wide clarity on the instrument's goals and scope early on will be important. A component of that is identifying a common level of ambition, recognising the usual push-pull that occurs in negotiating rooms, and the limitations of consensus-based decision-making.

At the time of writing, the precise goal of a future cyber PoA has not been identified. The current concept note outlines that the cyber PoA "is proposed to serve as a permanent, more structured yet flexible solution that allows for consensus driven, action oriented and transparent regular dialogue between States, more multi-stakeholder engagement and acknowledges the importance of capacity building and reliable coordinated efforts." This indicates that the initiative may currently be seen more as a way to create a permanent dialogue space or a process, than as an instrument, but doesn't give many further clues. The suggested title makes reference to state behaviour in cyberspace, which is a notable difference from the small arms UNPoA and its focus on illicit small arms trafficking, as conducted by criminal or non-state actors. The cyber security work at the UN is explicitly directed to developing norms of state conduct, which represents some progress.

While there is growing support for "human centric" approaches to cyber security within the OEWG, it's unlikely that the human cost of inter-state cyber operations will drive a cyber PoA process as it did in the case of small arms. Yet, some reflection on this and the relationship between international cyber security and the human rights frameworks on digital technology is warranted.

There is definitely an appetite for an instrument that will make a tangible difference; numerous governments and other stakeholders have expressed in the OEWG and other fora that the current voluntary norms are not sufficient.

Any scan of the daily news shows that aggressive action in cyber space continues to rise. Some of these countries are proponents of a legally binding instrument but recognise that the current political climate makes the prospects of one unlikely right now or are wary of lengthy negotiation processes. Others are staunch defenders of the norms and believe that they just need better implementation. In the OEWG, states and other actors have observed that despite the norms having been adopted by the entire UN membership, lack of awareness about them hampers implementation. This is a problem, and is where an open, inclusive, and transparent process to negotiate a new common framework will be important. When states have an active hand in shaping something, there is a greater likelihood of their ongoing support for and engagement with it.

Observation 2: A PoA can be an umbrella, and a springboard.

Flowing from the above sub-section about goals and objectives, the next set of questions relate to the potential substance of cyber PoA. Should it include provisions to curb, or prevent altogether, aggressive actions in cyber space? Will it include actions to prevent or remediate humanitarian harm from cyber operations and protect critical infrastructure? Will it have provisions that enhance building capacity and resilience, and cooperation? How specific and measurable will the actions be?

In theory, the cyber PoA could include action points relevant to all these areas, just as the small arms UNPoA includes activities falling under several core areas of arms control. The current cyber OEWG focuses on six standing thematic agenda items, which could potentially become the categories under which the cyber PoA's commitment are organised.[27]

The cyber PoA concept note sets out that the substantive basis of the instrument will be the acquis; the term being used increasingly to refer to the accumulated outcomes of different relevant processes—in particular the 2013 and 2015 GGEs on responsible state behaviour in cyber space; any outcomes that emerge from the sixth GGE and first OEWG that are now in session; and possibly the frameworks set out by non-UN processes, like the Paris Call for Trust and Security in Cyberspace[28] or the Global Commission for Stability in Cyberspace.[29] The concept note also states that "Consensus principles, recommendations and commitments could be added to that declaration, in order for the PoA declaration to be a standalone establishing document. The political declaration and subsequent implementation action should address International Law, Norms, Rules and Principles, CBMs and Capacity Building."[30]

Moreover, states have in the course of the GGEs universally acknowledged that existing international law exists in cyberspace. Which laws exactly, and when they apply, have yet to be articulated in detail by most governments though, and may add another layer of complexity to working out where and how a cyber PoA would fit into the current legal and normative landscape.

That said, the potential benefits of a cyber PoA pulling a diverse patchwork into a single instrument and framework is significant. It would make sense of a busy landscape and could clarify to states precisely what their—albeit voluntary, politically binding—commitments are, as well as the roles of other stakeholders.

There are many lessons to be learned from the small arms UNPoA about how it acted as an umbrella for existing initiatives, while later becoming a springboard for other agreements.

At the time when the small arms UNPoA was negotiated, there was already a patchwork of obligations and commitments relating to SALW, mainly regional. In some instances, these meant that there were pre-existing commitments that either needed to be accounted for in a new instrument, or that could provide a basis for the text of the new instrument. There were also other related instruments that were in the process of being negotiated at the same time. As one civil society expert has explained:

> In late October 1998, 16 states in West Africa signed a politically, but not legally, binding agreement to ban the production, import, and export of small arms for a three-year trial period. In addition, Western Hemisphere governments signed, and several ratified, a convention against the illicit manufacture and transfer of firearms. Preparations for the negotiation of a global protocol against firearms trafficking were begun. In addition, during the summer, the Canadian government proposed a treaty barring transfers of military-style small arms to insurgent forces and other non-state actors. And a December 1998 'Joint Action' of the Council of the EU committed all member-states to a set of principles concerning preventative (supply-side) and reductive (demand-side) measures.[31]

In the context of cyber security, where there is not only the acquis but also regional practices and standards to account for, the small arms UNPoA demonstrates the possibility of how a new instrument can pull such elements together. Some of the experts interviewed for this briefing paper cautioned against efforts to directly import text from other agreements, however—in this case, the 2013 and 2015 GGE outcome reports—without leaving space for negotiation. They stressed the importance of leaving open the possibility to articulate new language or commitments that address new concerns or realities that did not exist in 2013 or 2015.

Since its adoption, other agreements and processes have come into existence that seek to fill gaps in the small arms UNPoA or address dimensions of the same issue that have subsequently emerged as requiring attention. This includes the International Tracing Instrument (2005); the Geneva Declaration on Armed Violence (2006); the Arms Trade Treaty (2013); the Group of Governmental Experts on surplus ammunition stockpiles (2020); and numerous technical standards and guidelines. One expert interviewed for this paper explained that the UNPoA was "seminal in some ways, because it created forward motion in other areas"—although this same expert noted that these other areas were not necessarily the same ones that original UNPoA advocates wanted to see elevated.

Observation 3: Prioritise national implementation over international meetings.

At the outset of any cyber process, it will be important to understand that a programme of action is an instrument requiring implementation and not simply a discussion process in and of itself. A cyber PoA will likely mandate regular convenings that can constitute a dialogue opportunity for states and stakeholders, but those meetings must not supersede the importance of national and regional action to meet PoA commitments as a first priority.

The UNPoA on small arms is often criticised for not being well implemented at the national level while a disproportionate amount of attention and resourcing are given to its biennial meetings and review conferences. This has been the subject of extensive commentary from governments and non-governmental stakeholders over many years and in the process of preparing this briefing paper, it was the single most recommended "lesson" for cyber PoA advocates to consider. The same appears to be happening in the Arms

Trade Treaty process, where annual meetings discuss administrative matters while arms transfers around the world continue to result in human suffering.

The evidence for this critique has three major (and interrelated) sources: the real-world proof that small arms have continued to proliferate illicitly since 2001 with grave results; poor or uneven national implementation, as well reporting on implementation; and the often painfully divisive history of UNPoA international meetings.

The challenges that exist with respect to international UNPoA meetings, including its biennial meetings of states, or BMSs, and its review conferences, can be characterised as having two main sources: the topics on which states and stakeholders have chosen to focus discussion, and politicisation. The two are not unrelated.

Many of the same divisions that existed during the 2001 negotiations have lingered and at times dominated subsequent UNPoA meetings, limiting what can be discussed and decided. The UNPoA's first two biennial meetings of states, as well as its first review conference, failed to produce agreement on any substantive outcomes because of an inability to reach consensus. This spurred a decision to convene more focused and less political "meetings of governmental experts" in 2011, and 2015. In 2018, the final day of the UNPoA's Third Review Conference lasted a marathon 18 hours because of deep-rooted substantive differences of position as well as procedural delaying tactics and manoeuvring on the part of certain member states.[32]

As one ambassador observed already in 2012, "The process is yet to tackle seriously the challenge of effective implementation. And strong political cross-winds continue to prevent any meaningful discussions that might result in practical and effective improvements to small arms programmes in sensitive areas such as ensuring effective border controls and controls on small arms ammunition."[33]

Others have pointed out that some UNPoA meetings or documents have chosen to explore thematic topics that are not seen as core to its success. Writing in 2014 and 2015 respectively, both an original proponent of the UNPoA and a perennial critic made near identical observations that the UNPoA had lost its way and its meetings had become overly focused on peripheral issues. "If the small arms process was compared to that of food insecurity and malnutrition, it would be as if an initiative that once held the aspiration of eradicating world hunger had now become obsessed with food labeling and warehouse management."[34]

While it has been frustrating that the climate of UNPoA meetings has inhibited agreement, there is a twin issue about how "success" for those meetings is defined and understood. Overtime, the emphasis has fallen more to reviewing and adopting conference reports and documents than any true assessment of the instrument itself. "Adopting a document does not alone establish a positive outcome. The substance in the final outcome document would have to be quite strong to call the exercise a real success," wrote one civil society expert at the end of the Second Review Conference in 2012. Another observed, "But as this conference ends, we need to rededicate ourselves to making a difference 'on the ground' by focusing on reducing the human costs of armed violence. We can start by doing a thorough assessment of the accomplishments and failures of our efforts thus far. The Review Conference should have accomplished this task, but it did not do so. Now it's up to states and civil society to fill the gap."[35]

To be successful, a future cyber PoA will need to avoid this trap. One way to do so is for states to already begin identifying or exploring the types of national actions that would be triggered by potential components of a future cyber PoA—whether that be in the development of new national legislation or policy; engaging with other parts of their governments; budgetary changes; etc.

Another way is to deliberately design subsequent meetings as spaces to assess progress on meeting those commitments, identify mutual challenges, and share knowledge. This could be done by how the meetings are described in the text of the PoA and mandates they are given; and at a later stage, in how the programme of work and meeting agendas are designed.

The current cyber PoA concept note focuses a lot on future meetings and process, more so than substance. It already sets out suggestions for decision-making, participation, and periodicity—items that are usually agreed to after an instrument is adopted and sometimes even in the run-up to a first meeting. This is not to disparage those procedural dimensions; they lay the groundwork for all kinds of modalities that can influence the nature and tone of any given convening. But this does indicate that there is already a heavy emphasis on meeting cycles.

This may be because the proposal is only in its early days, and discussions of substance are more sensitive and will require discussion and consultation. It may also be because to date, all of the UN's forums on international cyber security are deliberative processes that have existed to create dialogue and exchange, rather than to take action.

Finally, cyber PoA supporters cannot afford to be naïve about the political climate in which the instrument may be negotiated and how those dynamics can impact the future. There are a few perennially contentious international cyber security issues where states have been at an impasse for years and general politicisation within international security is high, as evidenced by the creation of the two concurrent UN cyber processes (the GGE and the OEWG). An instrument that is overly preoccupied with outcome documents and meeting cycles will struggle to reach "success" in a contentious environment.

Observation 4: Make national reporting count.

The cyber PoA proposal includes a section about national reporting. Here, it is suggested that states could be encouraged to submit national implementation reports on a regular basis, every two years on a rotating basis (one report every three cycles, or six years) and potentially use a survey of national implementation that has been suggested by Australia and Mexico in the OEWG as a basis.[36]

Many instruments have some form of national reporting built into them as a way to foster transparency and accountability, as well as share experience and knowledge. Experience across these forums show that the general trend in reporting rates is either a decline over time or a lack of take-up at the outset, which sets a low bar of expectations. This is often worse when the instrument is not legally binding and reports are voluntary.

Reasons given for poor or declining reporting rates across the different disarmament fora that RCW monitors include reporting fatigue across multiple related forums; lack of capacity; need for, or problems with, a report template or method of submission; and unclear purpose or use of information contained in the reports.

The small arms UNPoA requests UN member states to voluntarily report on implementation. This commitment is further reiterated in the annual UNGA First Committee resolution on the illicit trafficking in of small arms.[37] Small arms UNPoA reports are submitted by the designated National Focal Point on small arms for each country—one of the action points contained in the UNPoA is the establishment of national focal points and of a national coordination body.

Over time, reporting rates have waxed and waned, and various steps have been taken to improve these rates and the quality of information being provided. "Given major shortcomings in the quality and frequency of national reporting and the lack of any comprehensive independent assessments, it is almost impossible to acquire an accurate picture of Programme of Action implementation and effectiveness," wrote one government official in 2008.[38] The outcome document of BMS3 in 2008 called for a biennial reporting cycle to reduce the reporting burden. Although a reporting template was not attached to the UNPoA in 2001, guidance was subsequently developed to assist states, and different templates have subsequently been prepared by the UN Office of Disarmament Affairs.[39]

Analysis shows that more reports are submitted in years when there is an international meeting and that reporting quality improved somewhat after the introduction of guidance and templates. Reporting rates vary by region, and the information that is included does not always paint a clear—or consistent—picture of overall implementation because of the variance in detail provided, which template is used, how states interpret questions within the template, etc.[40] Most analysis of the content of the reports has been done through civil society initiatives, sometimes jointly with UNIDIR, while UNODA maintains a website with all reports and some analysis.[41]

In the context of ICTs and cyber security, member states have, since 1998, been invited to submit voluntary national reports, which are compiled into an annual UNSG's report on ICTs.[42]

The cyber PoA proposal contains the suggestion that UNODA or UNIDIR "could be asked to analyse/synthesize the national reports to identify the core capacity challenges experienced by States in implementing the framework. This could also be presented and discussed in a roundtable with UN organizations, relevant multi-stakeholder platforms and non-UN based aid and development organizations." Encouraging an analysis or use for reports now could be helpful in offsetting grievances against mere "reporting for reporting's sake" and enable a true glimpse into national practice and impact of the instrument. However, analysis should go beyond an assessment of capacity challenges alone to general implementation of the instrument and state behaviour in cyber space. Public reporting would also enhance transparency and confidence between states.

In this vein, states could also seek to combine a PoA reporting provision with some of the proposals that have surfaced in the OEWG to improve accountability, such as peer review mechanisms. Diverse actors have raised concern that there is presently no accountability for complying with or implementing existing cyber norms. In order to not lose time in the years immediately following the adoption of a cyber PoA fumbling around over unresolved reporting-related questions, more discussion could take place on this topic in advance of the instrument entering negotiation.

In this area, cyber PoA proponents could learn not just from the small arms UNPoA but many other instruments as well, given that the same key questions around templates, frequency, purpose, method, public availability, and avoiding fatigue surface regularly across topics—and usually only after an instrument is agreed.

Observation 5: Engage non-governmental stakeholders meaningfully—and at all levels.

The participation of non-governmental stakeholders in the UN's international cyber security fora has been uniquely challenging. The original GGEs were closed, including to non-participating governments. When the OEWG was established and sold to the UN membership as an open and inclusive fora, hopes were high that this would also extend to meaningful participation of non-governmental experts and stakeholders, as outlined in the resolution establishing the group. Regrettably this has not been the case; a small and unnamed group of countries blocked the participation of any non-ECOSOC accredited civil society—including academia and industry—from both formal OEWG meetings, and all civil society from the informal consultations that have been occurring throughout the COVID-19 pandemic.[44]

This is highly unusual in international security and disarmament fora, especially those that emanate from the UNGA First Committee. While each one has somewhat different modalities for non-governmental participation—and likely varying levels of receptivity from governments to our inputs—it's very rare to categorically deny access in this way. The decision affected organisations, researchers, and private actors with demonstrated expertise and experience in the subject matter.

This situation has come under criticism from diverse governments participating in the OEWG, and non-governmental stakeholders have appealed it, too. It has fostered interesting collaborations and workarounds to ensure that stakeholder views are heard by governments. This included a three-day in-person informal stakeholder meeting in December 2019 at the UN, and a series of virtual dialogues that occurred in December 2020.[45]

Positively, the current cyber PoA proposal outlines diverse ways to allow for the "broad engagement" by relevant stakeholders. This includes around the ability to attend as well as deliver statements in future meetings, as well as noting a role for stakeholders in related initiatives that stem from the PoA such as capacity-building.

The small arms UNPoA offers a very different picture of non-governmental stakeholder involvement—as do most other processes on international security issues ranging from nuclear and autonomous weapons to the conventional arms trade.[46] While it cannot be said that stakeholder participation in all these fora is truly meaningful, there have not been the same obstacles to basic access that have existed within the OEWG.

In the years leading up to the adoption of the UNPoA, civil society played a central role in putting the issues of SALW proliferation on the UN agenda through sustained advocacy and research. Much of this focused on the human cost of proliferation, but some groups focused on technical aspects of small arms control. " By the start of the UN Small Arms Conference process in early 2000, it was clear to all involved that civil society could not be ignored. Its members had been conducting extensive research for several years, and as a result had produced a wide body of knowledge on the causes and consequences of the proliferation and misuse of small arms, as well as extensive policy recommendations on how to solve the problems associated with these weapons."[47]

Much of this was been coordinated through a single international civil society alliance, the International Action Network on Small Arms (IANSA), which has generated the establishment of national "ANSAs" in many countries, a women's network, and a secretariat. That said, pro-gun groups and shooting associations have also participated in many UN small arms meetings, often presenting opposing views to the vast majority of civil society.

Civil society was active and present throughout the intergovernmental process leading to the instrument's adoption:

> There were several focal points for integrating civil society into the process. Firstly, as states developed the issue through the UN system, NGOs were invited to make presentations and in some cases hold dialogue with states at the various experts panel meetings. Secondly, there was the question of how civil society would be integrated into the three Conference PrepComs and the final negotiating session in July 2001. In the end, NGOs made their presence felt in the form of presentations, briefings, and publication displays immediately outside the venues for these meetings at the UN. They also had significant interaction with state delegations, and in a few cases served on national delegations. Access to the meetings themselves was, however, limited to one morning session on 16 July 2001 of five-minute NGO presentations, representing both those supportive and critical of global action on small arms.[48]

n the years following the UNPoA's adoption, civil society took an active role in aspects of national UNPoA implementation. These derived somewhat from the two UNPoA references non-governmental stakeholders and encouragements to engage with them, but also an existing track record of collaboration.[49] A report published by the UNIDIR and the Small Arms Survey in 2010 takes stock of national implementation activities in the first ten years of the UNPoA's existence and cities many practical examples of civil society participation and collaboration with governments.[50]

At UNPoA meetings, civil society participation has manifested through a now familiar set of activities: joining expert panels; joining government delegations as experts; disseminating publications and materials; holding side events; and delivering presentations to the formal meetings. Much has been written and debated about if these kinds of activities count as "meaningful" civil society engagement or if they are now a tokenistic tradition—both in the context of the UNPoA as well as other fora—and also if civil society's ongoing participation in international UNPoA meetings inadvertently prop up or contributes to the process's malaise. This points to the importance of ensuring that civil society engagement is discussed early and often with all relevant stakeholders to ensure the ability of academics, activists, industry, and others to input meaningfully throughout the process.

The international cyber security stakeholder landscape is different than in SALW control. There is not a single alliance or coalition to unify hundreds of civil society organisations around a common goal. Many NGOs following the OEWG come from other issue areas: digital human rights, internet governance, disarmament, or cybercrime, and have varied ideas on the value of a cyber treaty or a cyber PoA, and priorities therein. There are many private sector actors, and a wide range within that sector among the roles they play and services they offer.

Yet, it is precisely this diversity that underscores the need for robust engagement with non-governmental stakeholders in a new PoA process. While a cyber PoA may govern state behaviour, state actions in the area of ICTs cannot help but collide with numerous other stakeholders—either as the owners, creators, or providers of technology; those with ability to investigate attacks and build resilience; or as individuals affected by state behaviour in cyberspace.

The constructive and generally well-accepted participation of non-governmental stakeholders in not only UNPoA meetings but also in the practical work of national and regional implementation offers a positive example for cyber PoA advocates.

This briefing paper has outlined five observations, or lessons, taken from the experience of the UN programme of action on small arms and light weapons that have relevance to the current proposal for a cyber PoA. These relate to establishing objectives and scope; understanding the broader normative and legal landscape; prioritising national implementational; national reporting; and meaningful engagement of non-governmental stakeholders.

Photo: CJ Dayrit / Unsplash

Recommendations

Building on these observations, WILPF puts forward the following recommendations:

- Build common agreement about the future instrument's scope and objectives through advance consultation and dialogue. Regional consultations, thematic consultations, preparatory committees, and having a platform for written inputs, are all ways to cultivate shared understandings ahead of a negotiating conference—as well as to ensure legitimacy, transparency, and widen buy-in into the process.

- Know that instruments and forums on international peace and security can successfully incorporate concerns about the human cost of weapons and violence, including gender dimensions—and that to be effective, they must do so. This has been demonstrated by the small arms UNPoA as well as other security and disarmament agreements that are motivated by a desire to alleviate human suffering and protect human rights.[51] The widening acceptability among member states in the OEWG about the importance of "human centric" approaches to cyber security and the human cost of cyber operations is a good first start that a cyber PoA should work to concretise.

- Identify how a cyber PoA can unite and solidify existing legal and normative frameworks in a way that brings clarity to the field rather than cluttering it further. Mapping out existing commitments and identifying where there is overlap and gaps is an important part of this process.

- Be ambitious. The prospect of any instrument's evolution is slim, and whatever loopholes exist when it is adopted are likely to remain. Rarely are instruments themselves updated, even if documents stemming from their future meetings reflect progress in thinking or technological change. Proponents of a cyber PoA should bear this in mind and seek to be as ambitious as possible at the outset towards creating a strong and effective agreement.

- Less talk, more action. As explained in this briefing paper, programmes of action set out tangible activities for its endorsers to implement at many different levels in order to reach a mutual goal. For a PoA to have impact, the commitments to action need to be prioritised. The conferences and meeting cycles mandated by an instrument are important for many things but should be designed in ways that will support implementation of the commitments contained in the instrument.

- Account for accountability. A cyber PoA could go a long way in filling the current accountability gap between the existing norms and actual practice by solidifying commitments and introducing reporting or review mechanisms. It will be crucial to incentivise reporting practices by making use of the information they contain or offering opportunities to discuss them, such as in mandated meetings.

- Engage non-governmental stakeholders. Their inclusion during the negotiation process lends legitimacy and can shape an instrument that will reflect lived realities and real threats. Moreover, given the nature of the cyber security field and ownership of key infrastructure and services, many different stakeholders will have an important role to play in implementing a cyber PoA.

Ultimately, political will is vital to the success of any instrument. While there is widespread condemnation of using cyberspace as a means or medium of violence, many states are not taking corresponding action to make such violence an impossibility.

Even while alarm bells are being raised about out-of-control state behaviour in cyberspace and a need for change, some of the most technologically advanced countries are adopting offensive cyber policies and closely integrating cyber operations into military strategies, under the guise of being "responsible" actors, in a narrative not unlike that used to justify nuclear weapon possession.

Cyber peace is not an elusive concept but a necessary goal. A cyber programme of action could become an important step on the road toward making cyber peace a reality by laying the groundwork to stop problematic cyber behaviour through tangible action, cooperation, nonviolence, and accountability.

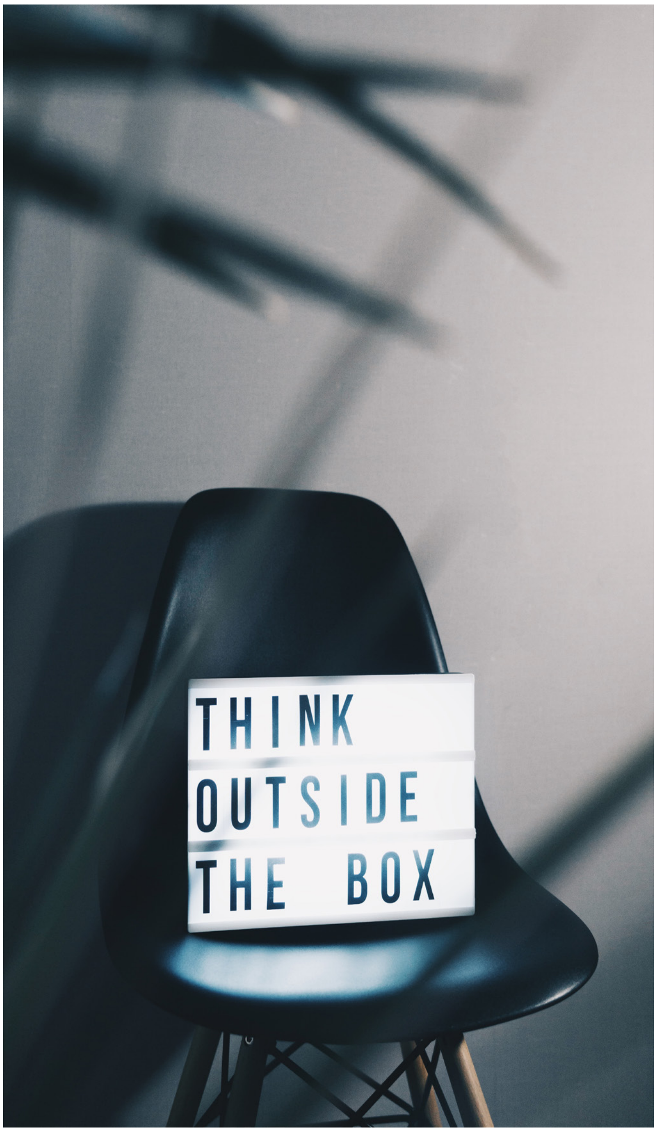

Photo: Nikita Kachanovsky / Unsplash

Endnotes

1 Reaching Critical Will began publishing the *Cyber Peace & Security Monitor* in 2019 to report on formal and open OEWG meetings. See https://reachingcriticalwill.org/disarmament-fora/ict/oewg/cyber-monitor.

2. Deborah Brown and Allison Pytlak, *Why gender matters in international cyber security*, WILPF and the Association for Progressive Communications, April 2020, https://reachingcriticalwill.org/images/documents/Publications/gender-cybersecurity.pdf.

3. Visit RCW's cyber peace and security fact sheet for more information https://reachingcriticalwill.org/resources/fact-sheets/critical-issues/14010-cyber-peace-and-security.

4. In particular, the author appreciates the inputs and reviews of Joseph Dube, Ed Laurance, Daniel Mack, and Paul Meyer; and to other civil society representatives who provided input anonymously.

5. "The future of discussions on ICTs and cyberspace at the UN," 30 October 2020, https://front.un-arm.org/wp-content/uploads/2020/10/joint-contribution-poa-the-future-of-cyber-discussions-at-the-un-10302020.pdf.

6. Ibid.

7. See "Cyber" in *First Committee Monitor 2020* No. 3 and *First Committee Monitor 2020* No. 5, Reaching Critical Will, https://reachingcriticalwill.org/disarmament-fora/unga/2020/fcm.

8. "The future of discussions on ICTs and cyberspace at the UN: Updated version," 2 December 2020, https://front.un-arm.org/wp-content/uploads/2020/12/joint-contribution-PoA-future-of-cyber-discussions-at-the-un-2-2-2020.pdf.

9. "Text proposed by the sponsors of the PoA," December 2020, https://front.un-arm.org/wp-content/uploads/2020/12/sponsors-oewg-report-text-proposal-final-12-2-2020.pdf.

10. UN General Assembly, *Draft Substantive Report [Zero Draft]*, January 2021, https://reachingcriticalwill.org/images/documents/Disarmament-fora/other/icts/oewg/documents/oewg-finalreport-substantive-zerodraft.pdf.

11. The December version of the proposal includes 47 governmental co-sponsors.

12. See "Cyber" in *First Committee Monitor 2020 No. 3* and *First Committee Monitor 2020 No. 5*, Reaching Critical Will, https://reachingcriticalwill.org/disarmament-fora/unga/2020/fcm.

13. The text of the Programme of Action is included within the Report of the United Nations Conference on the Illicit Trade in Small Arms and Light Weapons in All Its Aspects (A/CONF.192/15). Annexed to the report, after the instrument, is a list of the "Initiatives undertaken at the regional and subregional levels to address the illicit trade in small arms and light weapons" as well as a statement from the president of the Conference, in which he congratulates state on their achievement but also expresses certain disappointments.

14. Section II, para 33.

15. Lora Lumpe, "Curbing the Proliferation of Small Arms and Light Weapons," *Security Dialogue* 30, no. 2 (June 1999): 151–64, http://nisat.prio.org/Publications/Curbing-the-Proliferation-of-Small-Arms-and-Light-Weapons/.

16. Edward Laurance and Rachel Stohl, *Making Global Public Policy: The Case of Small Arms and Light Weapons*, Small Arms Survey, December 2002, 17, https://reliefweb.int/sites/reliefweb.int/files/resources/5108AD6B9C9F9F7AC1256D66004A3AC2-SAS-smallarmsandlightweapons-dec02.pdf.

17. UN General Assembly, *Resolutions Adopted By The General Assembly on the report of the First Committee*, 15 January 1996, A/Res/50/70, https://undocs.org/A/RES/50/70.

18. *Panel of Governmental Experts on Small Arms, Report*, A/52/298, August 1997, https://www.un-ilibrary.org/content/books/9789210584913c001/read.

19. Panel of Governmental Experts on Small Arms, Report, A/54/258, August 1999, https://www.un-ilibrary.org/content/books/9789210584913c002/read.

20. UN General Assembly, Resolutions Adopted By The General Assembly on the report of the First Committee, 12 January 1999, A/RES/53/77, http://www.poa-iss.org/CASAUpload/ELibrary/A-RES-53-77-E.pdf.

21. Matt Schroeder and Rachel Stohl, "Small Arms, Large Problem: The International Threat of Small Arms Proliferation and Misuse," *Arms Control Today*, June 2006, https://www.armscontrol.org/act/2006-06/features/small-arms-large-problem-international-threat-small-arms-proliferation-misuse.

22. Today, the UNPoA enjoys wide support from several institutions, including the UN regional centres on disarmament; the UN Office for Disarmament Affairs (UNODA) and a related coordination mechanism; various national and regional commissions on small arms; and has dedicated funding sources.

23. Lumpe, "Curbing the Proliferation".

24. Ibid.

25. Schroeder and Stohl.

26. Ibid.

27. These are Existing and potential threats; Rules, norms, and principles; International law; Confidence-building measures; Capacity building; and Regular institutional dialogue.

[28] The 2018 Paris Call for Trust and Security in Cyberspace is based around nine common principles to secure cyberspace. It is open to endorsement by states and civil society. See https://pariscall.international/en/.

[29] Learn more about the Global Commission on the Stability of Cyberspace's work on cyber norms at https://cyberstability.org/norms/.

[30] *Cyber PoA Concept* note https://front.un-arm.org/wp-content/uploads/2020/12/sponsors-oewg-concept-note-final-12-2-2020.pdf.

[31] Lumpe, "Curbing the Proliferation."

[32] Allison Pytlak, "Inside the theatre of the absurd—the final day of RevCon3", *Small Arms Monitor 10, no. 6* (3 July 2018), https://reachingcriticalwill.org/disarmament-fora/salw/2018-rev-con/small-arms-monitor/12669-small-arms-monitor-vol-10-no-6.

[32] Jim McLay, *2012 and Beyond: Advocacy and Action in the UN Small Arms Process*, Small Arms Survey, August 2012, p.3, http://www.smallarmssurvey.org/fileadmin/docs/G-Issue-briefs/SAS-BP2-2012-and-beyond.pdf.

[33] Daniel Mack and Guy Lamb, "Firing Blanks: The Growing Irrelevance of the UN Small Arms Process", IPI Global Observatory, https://theglobalobservatory.org/2014/08/firing-blanks-growing-irrelevance-un-small-arms-process/.

[34] Dr. Natalie Goldring, "Measuring the effectiveness of the PoA," *Small Arms Monitor: The Blog*, 10 September 2012, https://smallarmsmonitor.blogspot.com/2012/09/measuring-effectiveness-of-poa.html.

[35] "Joint Proposal: 1 National Survey of Implementation of United Nations General Assembly Resolution 70/237", December 2020, https://front.un-arm.org/wp-content/uploads/2020/12/updated-december-2020-draft-v02-joint-oewg-proposal-survey-national-implementation.pdf.

[36] "The illicit trade in small arms and light weapons in all its aspects", A/C.1/75/L.4, 13 October 2020, https://reachingcriticalwill.org/images/documents/Disarmament-fora/1com/1com20/resolutions/L44.pdf.

[37] McLay, 2012 and Beyond, 3.

[38] McLay, 2012 and Beyond.

[39] Paul Holtom and Moshe Ben Hamo Yeger, *Implementing the Programme Of Action and International Tracing Instrument: An Assessment of National Reports, 2012–17*, Small Arms Survey, June 2018, http://www.smallarmssurvey.org/fileadmin/docs/U-Reports/SAS-Report-PoA-ITI-2012-17.pdf.

[40] See https://smallarms.un-arm.org/.

[41] See https://www.un.org/disarmament/ict-security/.

[42] "Proposal: States Cyber Peer Review Mechanism" for state-conducted foreign cyber operations, ICT4Peace, https://unoda-web.s3.amazonaws.com/wp-content/uploads/2020/03/ict4p-peace-proposed-states-cyber-peer-review-3.pdf.

[43] UN Office for Disarmament Affairs, "Outcome of non-objection procedure for attendance of non-governmental organizations at the Open-ended Working Group meeting (9-13 September 2019)," 29 August 2019, https://reachingcriticalwill.org/images/documents/Disarmament-fora/other/icts/oewg/documents/note-verbale-ict-ngos.pdf.

[44] See https://www.un.org/disarmament/oewg-informal-multi-stakeholder-meeting-2-4-december-2019/ and https://letstalkcyber.org/. Reaching Critical Will has also reported on the December 2019 meeting through its publication, the *Cyber Peace & Security Monitor* available at https://reachingcriticalwill.org/disarmament-fora/ict/oewg/cyber-monitor.

[45] Sheetal Kumar and Allison Pytlak, *NGO Participation in Multilateral and Multistakeholder Forums: Good Practice Examples*, Global Partners Digital, 23 June 2020, https://www.gp-digital.org/publication/ngo-participation-in-multilateral-and-multistakeholder-forums-good-practice-examples/.

[46] Laurance and Stohl, *Making Global Public Policy*, 17.

[47] Ibid., p.18.

[48] See UNPoA, Section II, paragraph 40 and Section IV, paragraph 2(c).

[49] Sarah Parker and Katherine Green, *A Decade of Implementing the United Nations Programme of Action on Small Arms and Light Weapons*, Small Arms Survey and UNIDIR, 2012,https://www.unidir.org/files/publications/pdfs/a-decade-of-implementing-the-unpoa-analysis-of-national-reports-en-301.pdf.

[50] These include the Convention on the Prohibition of the Use, Stockpiling, Production and Transfer of Anti-Personnel Mines and on their Destruction; the Convention on Cluster Munitions; the Arms Trade Treaty; and the Treaty on the Prohibition of Nuclear Weapons.

Reaching Critical Will

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

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 for an end to war, militarism, and violence. It also investigates and exposes patriarchal and gendered aspects of weapons and war.

We monitor and analyse international processes and work in coalitions with other civil society groups to achieve change, provide timely and accurate reporting on all relevant conferences and initiatives so that those unable to attend can stay informed, and to maintain a comprehensive online archive of all statements, resolutions, and other primary documents on disarmament.

Reaching Critical Will also produces research studies, reports, statements, fact sheets, and other publications on key issues relevant to disarmament, arms control, and militarism.

www.reachingcriticalwill.org
disarm@wilpf.org