UNIDIR
UNITED NATIONS INSTITUTE FOR DISARMAMENT RESEARCH

Preventing and Mitigating ICT-Related Conflict

Cyber Stability Conference 2018

Summary Report

UNIDIR RESOURCES

Acknowledgements

Support from UNIDIR core funders provides the foundation for all of the Institute's activities. This conference was supported by the Governments of France, Germany and the Russian Federation.

This report was drafted by Dr Camino Kavanagh, non-resident researcher at UNIDIR.

About UNIDIR

The United Nations Institute for Disarmament Research (UNIDIR)—an autonomous institute within the United Nations—conducts research on disarmament and security. UNIDIR is based in Geneva, Switzerland, the centre for bilateral and multilateral disarmament and non-proliferation negotiations, and home of the Conference on Disarmament. The Institute explores current issues pertaining to a variety of existing and future armaments, as well as global diplomacy and local tensions and conflicts. Working with researchers, diplomats, government officials, NGOs and other institutions since 1980, UNIDIR acts as a bridge between the research community and Governments. UNIDIR activities are funded by contributions from Governments and donor foundations.

Note

The designations employed and the presentation of the material in this publication do not imply the expression of any opinion whatsoever on the part of the Secretariat of the United Nations concerning the legal status of any country, territory, city or area, or of its authorities, or concerning the delimitation of its frontiers or boundaries. The views expressed in the publication are the sole responsibility of the individual authors. They do not necessary reflect the views or opinions of the United Nations, UNIDIR, its staff members or sponsors.

www.unidir.org

Contents

List of acronyms and abbreviations

APT	Advanced persistent threats
CBMs	Confidence-building measures
GGE	Group of Governmental Experts
ICAO	International Civil Aviation Organization
ICT	Information and Communications Technologies
IoT	Internet of Things
IVEP	International Vulnerabilities Equities Process
UN	United Nations
UNIDIR	United Nations Institute for Disarmament Research
VEP	Vulnerabilities Equities Process

1 Introduction

"We are living in dangerous times". This simple yet stark message, conveyed by the UN Secretary-General upon the release of his Disarmament Agenda[1] in May 2018, reflects an era of converging global challenges. A diminishing respect for international norms and institutions and a growing trust deficit is challenging the post-War international order. Competition for power and influence across all strategic environments is giving rise to increasing instability.

Against this backdrop, destabilizing activities involving the use of Information and Communications Technologies (ICT) by State and non-State actors is of deepening concern. States have repeatedly asserted that managing the escalatory potential of these activities and the uncertainties surrounding them is a core objective of the international community. In response, they have pushed for more predictable and responsible behaviours; mechanisms that can build trust and confidence between States, manage crisis and prevent conflict; and more resilient and secure technologies. This notwithstanding, the gap between our collective aspirations and the practice and behaviours of States and other actors seems to be widening. This gap poses real threats for international security: investing in efforts to narrow it is an urgent priority.

Identifying options and pathways to prevent and mitigate ICT-related conflict was the focus of UNIDIR's 2018 Cyber Stability Conference, held in Geneva on 26 September 2018. The conference brought together representatives from government, the private sector, academia and civil society to explore current State strategy and practice; developments at regional level; private sector engagement; and prospects for reinvigorating multilateral engagement to address the growing threat of ICT-related conflict. Through the lens of these different topics, the conference looked at the widening gap between our collective aspirations and State practice, identifying different approaches involving different actors to narrowing it.

This summary report identifies the main issues discussed as well as key take-aways from the conference. Recordings of the presentations are available on UNIDIR's website. Discussions at the meeting were conducted under Chatham House Rule.

[1] *Securing Our Common Future: An Agenda for Disarmament,* The United Nations Office for Disarmament Affairs, 2018.

2 Summary of Discussions

PREVENTING AND MITIGATING THE RISK OF CONFLICT STEMMING FROM THE MALICIOUS USE OF ICT: INSIGHTS INTO CURRENT STATE STRATEGY AND PRACTICE

Mind the Gap!

The widening gap between the collective aspirations of the international community regarding security and stability on the one hand, and the actual practices of States on the other was a central theme of the conference. There is a sharp disconnect between what States commit to in fora such as the UN Groups of Governmental Experts (GGEs), regional and sectoral fora and what intelligence and military services are reportedly authorized to do in the name of national security. Narrowing this gap should be a key priority for all States.

Against this context, participants discussed a number of intertwined ICT-related insecurity dilemmas, including those of a national security, technological and commercial character, which pose serious risks to international and regional security and stability. Many of these are hard to separate from broader non-ICT related challenges currently affecting relations among States and between States and other actors. Deepening understanding of the inter-connected nature of these insecurity dilemmas is crucial for any strategy aimed at reducing the risk of conflict, yet the tools to do so are far from mature; the information required is not always accessible; the incentives are not always evident; and the parties needed to shape solutions are not always invited or available.

REGIONAL OPPORTUNITIES AND MECHANISMS TO PREVENT AND MITIGATE CONFLICT

Bridging the Gap

Important efforts are underway at the regional level to prevent and mitigate conflict stemming from the malicious use of ICT. Participants specifically discussed efforts by regional organizations to promote and implement the norms and confidence-building measures (CBMs) recommended by the GGEs and to facilitate cooperation between States in managing immediate crises as well as medium- and longer-term risk. Divergences in perceptions of threats and risk, and in capacities and resources within and across countries and regions, pose serious challenges to putting in place the requisite mechanisms and measures.

Nonetheless, progress is being made across regions, notably where certain cooperative and transparency measures are concerned. Showcasing that progress, and deriving and sharing lessons from specific experiences, is important for building trust. In some instances, a significant breach by criminal actors or conflict dynamics whereby one country has been the target of another country's offensive activities, have necessitated a steep learning curve in the technical and policy realms and have driven the allocation of resources. Distilling and sharing lessons from these experiences is important. Moving forward, a sustained effort to build up the necessary policy and technical capacity, including via regional organizations, the technical community and industry actors, remains crucial, as does the allocation of adequate resources. These steps can contribute significantly to bridging the gap between our international security goals and actual practice.

THE ROLE OF THE PRIVATE SECTOR IN COUNTERING THE PROLIFERATION OF MALICIOUS ICT CAPABILITIES, TOOLS AND TECHNIQUES

Securing the Gap

States are not the only actors with responsibilities when it comes to cyberspace and international security. Private sector actors, too, are increasingly expected to shoulder responsibilities, particularly with regard to countering the spread of malicious ICT capabilities, tools and techniques. Participants discussed the evolving nature of the latter and some of the dynamics—market, national security and other—enabling their spread. Importantly, they highlighted some of the structural issues relating to the technology sector that continue to pose serious risks. For some participants, confronting these structural issues from a security and resilience perspective would help strengthen defence and would be a much more effective, sustainable and stable basis for dealing with malicious tools, techniques and activity than the current trend of serial patching and offensive posturing.

A number of industry actors are promoting initiatives to enhance security of ICT services and products, strengthen resilience and ensure their peaceful use. The challenge will be to both scale and frame them within a broader information assurance policy framework at national and international levels. The conference discussed a new government-backed initiative aiming to bring different actors under one umbrella and promote coherence and consistency of effort (the Paris Roadmap for Trust and Security in Cyberspace).[2] Also presented was a proposal for a technology norm—an International Vulnerability Equities Process. By focusing on strengthening the overall security and resilience of technology products and services, the proposed norm would help contain the spread of vulnerabilities and their malicious use, and shift the current focus from offense to defence.

MULTILATERAL PROCESSES AND SYNERGIES ACROSS INITIATIVES: LOOKING AHEAD

Negotiating the Gap

The discussion around existing processes and initiatives centred largely on our shared responsibility of—and mutual interest in—contributing to international stability and security through actions in cyberspace. For many, establishing patterns—or even a culture—of responsible State behaviour can help generate trust and improve transparency. History has shown that practical measures such as establishing channels for communication and information sharing help reduce the risk of conflict. Greater clarity of how existing rules can be applied can help foster their adherence and identify where new rules might be required. Nonetheless, the fact that the legitimacy of the post-Cold War rules-based order is eroding poses a serious challenge to the emergence of a rules-based culture in this area.

To tackle the growing gap, participants considered potential next steps within the UN to build on the work of previous GGEs as well as a number of complementary initiatives. A proposal for a draft resolution was also discussed.[3] Diverging views on the work of the GGEs and how to carry the discussions forward were sharply evident. Despite these divergences, there was wide agreement about the need to continue expert discussions within the framework of the UN, although getting to yes on the 'what' and the 'how' will be challenging. In this respect, all eyes are on the UN General Assembly First Committee deliberations in October.

[2] The proposal was presented by France in the form of a non-paper. The initiative will be formally launched during Paris Peace Forum in November 2018.

[3] The proposal was described in a statement by the Russian Federation presented during the Conference.

3 Key take-aways

NORMS AND THE MULTILATERAL PROCESS

Significant emphasis was placed on the **importance of both operationalizing and universalizing the framework** (or package agreement) that has emerged from multilateral efforts over the past two decades. The core elements of this framework stem from the work of the GGEs on international law, non-binding norms, rules and principles for the responsible behaviour of States, and confidence, cooperative and capacity building measures.

Without clarity and transparency of action and the requisite capacities and resources, progress on implementing the recommendations of the GGEs will remain fitful. Closing these gaps is therefore crucial. To this end, some participants stressed the **need for greater clarity on how States apply existing international law and norms of behaviour in cyberspace**. There are several ways to do this: through national statements and national policy and strategy; through the promotion and development of CBMs via regional groups and targeted capacity-building programmes; and through reporting or dialogue at the UN.

For some participants, the focus on operationalization is misguided, and additional work needs to be done to develop more universal norms, rules and principles under the auspices of the UN. A specific proposal for a new First Committee resolution was presented. Framed as a code of conduct, it draws language from some of the GGE reports, as well as language from other documents.

For others, operationalizing and universalizing the work of the GGEs involves responding to the UN General Assembly's call for **States to be guided in their use of ICT by the report of the 2015 GGE and the recommendations therein**. Some participants pressed home the urgency of this call, noting that the failure of States to adhere to the norms recommended by the GGE is driving the growing reliance on offensive capabilities and increasing instability internationally. Implementing the GGE recommendations can help reduce risk and identify gaps in the existing normative framework, build trust, raise awareness and draw others in. Many expressed that any new GGE should build on existing work and should include mechanisms for consultations with the broader UN membership as well as other key stakeholders.

Despite divergences of opinion over a number of issues, there was strong support among participants about **the importance of the GGE process per se and its value as a channel for expert dialogue, as well as the urgency of moving the dialogue forward**. In this regard, several government representatives signalled their desire for a new GGE.

Given current tensions between States and the hardening of positions between different groups of States, some participants questioned whether a new GGE could be productive. **Ensuring an environment that is conducive to expert talks and to building trust remains a significant challenge.**

STATE STRATEGY AND PRACTICE

Participants noted **the importance of national doctrine and strategy and declaratory statements,** including for national coordination and broader transparency and accountability purposes.

Some States have revised their policies and strategies to **integrate consequences aimed at deterring or punishing unacceptable behaviour in cyberspace.** To date, these consequences range from "naming and shaming" malicious actors, to indictments and sanctions.

The conference discussed the **risks posed by the current shift to more offensive military postures in lieu of strategies centred on defence, security and resilience, risk management and the promotion of norms of restraint**. Concerns raised relate primarily to the fact that strategies weighted towards offense can drive reciprocal action in the form of tit-for-tat escalation, which political institutions may not have the ability to contain. For many participants, this shift in strategy contradicts the stabilizing objectives of the GGE recommendations, as well as the thrust of many national cyber or digital security strategies and associated political statements.

CRISIS MANAGEMENT AND CONFLICT PREVENTION

Signalling—a key tool of strategic deterrence—was highlighted as an important element of conflict prevention. Yet, **signalling in this environment is complicated by a number of uncertainties,** including about:

- the offensive capabilities of other States and their willingness to use them;
- the alleged precision of the tools and related difficulties in calibrating their effects, which in turn challenges the ability to shape a proportionate response; and
- the lifecycle of the tools—reverse engineering of offensive tools can either render the tools useless or facilitate their spread, depending on the time it takes to fix the vulnerability that has been exploited.

In short, many participants view deterrence in the cyber realm as either misapplied or lacking maturity and as a result high risk and potentially destabilizing.

At the multilateral level, **a number of crisis management and confidence-building mechanisms are slowly maturing**. Decision makers are increasingly aware of the importance of the ICT/cyber dimension in the event of a crisis or conflict. They understand the need to bolster existing mechanisms, so as to strengthen trust and cooperation between States, and avoid or manage escalation. Underpinning these mechanisms with secure and resilient components and systems, as well as the requisite capacities and resources, is crucial.

Progress in operationalizing these mechanisms differs significantly within and across regions. In some regions where institutions and trust are strong and resources readily available, a number of mechanisms are already in place. Other regions have had to prioritize, focusing on basic measures such as points-of-contact or bilateral cooperation agreements for incident response purposes and to facilitate information sharing. In some cases, these mechanisms have been put in place only after a serious incident has occurred. In other cases, the absence of conflict or serious ICT incidents inhibits prioritization and the allocation of adequate resources. The experiences of States that have managed major incidents are important for strengthening policy and technical expertise in other countries.

In the future it will be **important to ensure that all regional organizations have some form of working group for discussing CBMs and crisis management**, as well as obstacles to their effective implementation. Enabling cooperation across these working groups will be equally important given the global nature of the challenges at hand.

At the bilateral level, developments both within and beyond the ICT environment are making it increasingly difficult to open and sustain channels of dialogue and engagement. **Targeted and tailored crisis management mechanisms between appropriate diplomatic and/or military counterparts are lacking.** For some participants, the major powers bear a large proportion of responsibility for ensuring their actions do not lead to conflict. Participants drew important

inferences for crisis management and confidence building from existing bilateral agreements[4], while cautioning about the limitations of applying them to the ICT environment.

Ensuring that crisis management and conflict prevention tools remain adaptable and responsive to the current international context is critical; as is avoiding the politicization of such mechanisms, so they are allowed to mature and so trust between parties can grow. In addition, any mechanism created will only be robust if it is understood, accepted, internalized, and implemented.

Needless to say, **not all States view State-on-State ICT-related conflict as their most pressing priority.** At the same time, the reality that their territory might be used to conduct or route malicious ICT activity could unwittingly involve them in a situation of escalating tensions for which they need to prepare. Basic preparedness is also crucial for dealing with incidents outside the realm of conflict and in this, the private sector and technical experts and associations play a crucial role.

GOVERNANCE

A key theme discussed throughout the day was the inadequacy of our institutions—national, sub-national and multilateral—and our policy tools for dealing with the nature of the challenges we have to confront. The challenge of keeping pace with advances in technology is even greater as different technologies advance and converge, creating novel challenges for our societies. The disparities in our populations and national contexts make it difficult to shape policies that respond to the interests of everyone. More sustained discussion of the adaptability of domestic and global institutions and policy instruments to current technological realities is crucial.

At the international level, **the absence of any formal governance structure for this area was also raised as a challenge**. Since the early 2000s, most societies have undergone rapid digitalization. Ensuring predictability or trust in the infrastructure on which the increasingly digitalized global economy is sustained is therefore a critical component of international security and stability. In the absence of a global governance structure in this area, participants discussed the feasibility of establishing a hybrid structure similar to the International Civil Aviation Organization (ICAO)—which has a consultative mechanism with its private sector equivalent.

TECHNOLOGY DILEMMAS AND THE PRIVATE SECTOR

Participants highlighted a number of trends stemming from the vulnerabilities in ICT products and services. These include the rise in advanced persistent threats (APT) by both State and non-State actors from all corners of the world; the growing professionalization of illicit activity online, which now involves serious organized crime and mafia groups who exchange business models and information, and compete for access to and provision of services; increasing attacks on industrial control systems; an increase in the number of botnets running on devices that form part of the "Internet of Things" (IoT) and most of which are insecure by design; and, of course, their potential exploitation by intelligence and military services for offensive purposes.

The private sector plays a crucial role in responding to these developments. For instance, experiences from the energy sector have demonstrated that effective collaboration between government and the private sector is both crucial and possible and that such collaboration can be anchored in clear policy and a clear definition of roles and responsibilities.

---

[4] Examples of such agreements include: the Agreement on the prevention of incidents at sea (1972); the Agreement on the prevention of nuclear war (1973); the Agreement on the prevention of dangerous military activities (late 1989) between militaries; and the more recent MoU on the prevention of flight safety incidents in Syria (2015).

Discussions throughout the day laid bare that **it is impossible to talk about security and stability and reducing the risk of conflict without taking a serious look at the ICT sector itself**. Today, even the most secure computer operating systems pose risks once they are networked. Highly vulnerable components of ICT products drive exponential problems as the technologies become integrated into societies. These engines of vulnerability spread through the capital goods sector into critical infrastructures and government and enterprise computing, while business models are based on off-loading risk downstream.

Some companies are taking important steps to ensure greater security of their products and services.[5] Yet, these initiatives tend to be fragmented, adopted by only a few companies and only in some settings. Nonetheless, **some initial efforts to provide the policy framing, incentives and disincentives required to induce a broader shift to security and resilience in the ICT market are underway.**

In this regard, **participants discussed a suggestion for a technology norm that would raise information assurance so as to reduce vulnerabilities and moderate the insecurity dilemmas affecting the international community**. Such an approach would reduce the possibility of using vulnerabilities for offensive purposes and shift the balance to defence. The framework for implementing the norm is an International Vulnerabilities Equities Process (IVEP), which builds on national level VEPs. In addition to identifying relevant actors and responsibilities, organizational modes and priorities, it identifies some of the national policy levers for incentivizing better information assurance and resilience and building a trusted architecture; and how existing public and private mechanisms can be used to implement the norm internationally.

Other technology-related dilemmas discussed during the conference centred on the IoT and developments in different sub-fields of artificial intelligence, each of which pose serious risks to security and stability for which we are not yet prepared in policy, normative or operational terms. More targeted discussion on these risks and their links to the broader international cyber security and stability debates are urgently required.

ROLES AND RESPONSIBILITIES

Undoubtedly **States carry primary responsibility for national security**. The latter is underpinned by responsibilities towards their citizens (public safety, privacy and other rights) and with regard to other States. At the same time, **discussions exposed the important roles and responsibilities of other actors in strengthening security and stability within and beyond national borders.** The UN GGE reports provide several entry points for this engagement, as do many other initiatives.

[5] For example, Norilsk Nickel's critical infrastructure initiative; Microsoft's Tech Accord, Siemen's Charter of Trust, Kaspersky's Transparency Initiative.

Annex 1
Agenda

Welcome and Opening Remarks

Michael Møller, Director-General, United Nations Office at Geneva
Renata Dwan, Director, UNIDIR

Session 1. Preventing and Mitigating the Risk of Conflict Stemming from the Malicious Use of ICT: Insights into Current State Strategy and Practice

Moderator — Sean Kanuck, Director of Cyber, Space and Future Conflict, The International Institute for Strategic Studies

- Chuanying Lu, Senior Fellow, Institute for Global Governance Studies, Shanghai Institute for International Studies
- Michelle Price, Chief Executive Officer, AustCyber
- Oleg Shakirov, Expert on Foreign Policy and Security, Center for Strategic Research
- Rafal Rohozinski, Chief Executive Officer, The SecDev Group

Session 2. Regional Opportunities and Mechanisms to Prevent and Mitigate Cyber Conflict

Moderator — Paul Cornish, Associate Director, Oxford Martin Fellow, The Global Cyber Security Capacity Centre

- Katherine Getao, ICT Secretary, Ministry of ICT of Kenya
- Nato Goderdzishvili, Head of Legal Department, LEPL Data Exchange Agency, Ministry of Justice of Georgia
- Heli Tiirmaa-Klaar, Ambassador for Cyber Diplomacy, Ministry of Foreign Affairs of Estonia
- Pablo Hinojosa, Strategic Engagement Director, Asia-Pacific Network Information Centre

Session 3. The Role of the Private Sector in Countering the Proliferation of Malicious ICT Capabilities, Tools and Techniques

Moderator — Kerstin Vignard, Deputy Director and Chief of Operations, UNIDIR

- John Mallery, Research Affiliate, Computer Science & Artificial Intelligence Laboratory, Massachusetts Institute of Technology
- Nicolas Mazzucchi, Research Fellow, Fondation pour la Recherche Stratégique
- Liga Rozentale, Director of Cybersecurity Policy, Europe, Microsoft
- Anton Shingarev, Vice President for Public Affairs, Kaspersky Lab

Session 4. Multilateral Processes and Synergies Across Initiatives: Looking Ahead

Moderator — Camino Kavanagh, Senior Visiting Fellow, Department of War Studies, King's College London

- Joe Preston, Head of Cyber Diplomacy (Governance & International Law), Cyber Policy Department, National Security Directorate, Foreign and Commonwealth Office, United Kingdom of Great Britain and Northern Ireland

- Nadezhda Sokolova, Expert on International Information Security, Department for New Challenges and Threats, Ministry of Foreign Affairs of the Russian Federation
- Carmen Gonsalves, Head, International Cyber Policy, Security Policy Department, Ministry of Foreign Affairs of the Kingdom of the Netherlands
- Amandeep Singh Gill, Executive Director, Secretariat of the High-Level Panel on Digital Cooperation

Concluding Remarks

UNIDIR
UNITED NATIONS INSTITUTE FOR DISARMAMENT RESEARCH

Preventing and Mitigating ICT-Related Conflict

Cyber Stability Conference 2018

Summary Report

Identifying options and pathways to prevent and mitigate ICT-related conflict was the focus of UNIDIR's 2018 Cyber Stability Conference, held in Geneva on 26 September 2018. The conference brought together representatives from government, the private sector, academia and civil society to explore current State strategy and practice; developments at regional level; private sector engagement; and prospects for reinvigorating multilateral engagement to address the growing threat of ICT-related conflict. Through the lens of these different topics, the conference looked at the widening gap between our collective aspirations and State practice, identifying different approaches involving different actors to narrowing it.

UNIDIR RESOURCES