UNIDIR RESOURCES

UNIDIR Cyber Security Conference 2012 (CS12)

The Role of CBMs in Assuring Cyber Stability

The United Nations Institute for Disarmament Research (UNIDIR) held its inaugural Cyber Security Conference (CS12) entitled "The Role of Confidence-Building Measures in Assuring Cyber Stability" on 8–9 November 2012 in the Palais des Nations in Geneva. The event was carried out in partnership with Chatham House and the Verification Research, Training and Information Centre (VERTIC), with funding support from the governments of Germany and the United States of America. The aim of the event was to share knowledge and generate discussion on the cyber domain and the role that confidence-building measures (CBMs) might play in encouraging and nurturing both security and stability. The event comprised seven panels, with presentations taking place on the record, and subsequent question and answer sessions taking place under the Chatham House Rule.

Framing the discussion

Cybersecurity and stability is a cross-cutting issue that concerns a diverse spectrum of stakeholders, and the cyber domain plays a critical part in an enormous range of daily human activities, including communications, commerce, international security, and financial transactions. Society's reliance on the cyber domain is already widespread and only likely to increase. Therefore, the enormous transformative and economic benefits made possible by such technology demand that it be considered an important resource for all. As such, preserving the utility of the cyber environment and preventing misuse should be a common goal for all stakeholders, in government, the military, civil society, and the private sector.

In dealing with a topic as broad as cyber stability, it is necessary to set clear conceptual boundaries to narrow the scope of the discourse. In the opening remarks of this inaugural UNIDIR cyber stability conference, **Theresa Hitchens** framed the subsequent discussions by underlining that the emphasis at CS12 would be placed on the international security aspect of the cyber domain, and how the international community might deal with the issue of cybersecurity through multilateral efforts. This focus ensured a spotlight on state-to-state activities and state–proxy–state activities, rather than encouraging narrow discussions on cybercrime or cyberterrorism. UNIDIR's aims, reflected in the conference structure and format, were instead to broaden the international security debate both geographically and across stakeholders, while showcasing how CBMs could be a valuable tool for progress.

The panels covered a wide range of topics, although discussions often centred around a number of recurring themes. The most pertinent of these are summarized in section I, while section II provides a digest of each of the individual presentations delivered at the event.

Section I

Panel 1
CBMs: concepts and applications

Gotz Neuneck opened the panel with a discussion of the applicability of trust- and confidence-building measures to the cyber domain. He underlined that, as cybersecurity is such a broad subject, no single state could deal with these issues alone; it will require international cooperation and the participation of civil society, non-governmental organizations (NGOs), and other stakeholders. He noted that while there are legitimate and illegitimate uses of kinetic weapons, it is unclear what legitimacy and illegitimacy might look like in cyberspace as information and communication technologies (ICTs) are highly dual-use, making it hard to distinguish between military and civilian purposes. Neuneck also questioned how one can distinguish between defence and offence in a cyber context, concluding that definitions are likely to be complicated. All of these issues appear to be difficult challenges for the development of future legal and policy initiatives in the cyber domain.

In light of these concerns, Neuneck suggested that a culture of confidence should be encouraged, and went on to discuss the possible applicability of CBMs in the cyber context. He described the potential benefits of CBMs including effective détente, increased predictability, protection of infrastructure, and improvement in state-to-state relationships, which might provide a platform for further cooperation. Nevertheless, simply "cutting and pasting" pre-existing CBMs from other fields was cautioned against, as the nuances of cyber technology render ideas like effective verification or de-militarized zones impractical. It was suggested that the development of best practices and a common lexicon to discuss cybersecurity would be sensible starting points, as well as other risk reduction measures such as regional or global early-warning mechanisms for attacks and capacity-building.

Following that introduction, **Nathalie Weizmann** examined how international humanitarian law (IHL) relates to cyberwarfare. In her opinion, it is clear that due to a number of factors, IHL is not unequivocally applicable to the cyber domain. While the discussions did not reject the possibility of IHL being applied in some way to cyber activities, the lack of clarity certainly added weight to the argument for the consideration of CBMs as a more workable alternative.

As a first threshold for IHL to apply, Weizmann noted that one needs to confirm whether a state of armed conflict exists. However, this is problematic to establish in the cyber domain due to the difficulty of accurately attributing an attack to a specific actor. Hypothetically, if it were possible to establish that a state of armed conflict existed and therefore IHL could be applied, she suggested some key rules that would need to be considered in the context. First, IHL asserts that means and methods of warfare are not unlimited, and prohibits the use of weapons that cause superfluous injury or that are by their nature indiscriminate. Weizmann noted this aspect of IHL would certainly have implications for cyber technologies that were indiscriminate in their nature.

Weizmann also highlighted the concept of military utility—that a military actor must limit targets to military objectives. Given the dual-use nature of cyberspace and technology,

the distinction becomes unclear. Some would say that marginal military use would suffice as a qualifying threshold; if this were true it may render this particular aspect of IHL untenable for the cyber domain. Weizmann summarized by conceding that while there are interesting possibilities in considering cyberattack from an IHL perspective, it might be impossible to establish if IHL applied to an attack in cyberspace, and in any case it would be very difficult to ensure compliance with the fundamental rules of IHL.

Panel 2
Technical and political challenges to cyber stability

The second panel began with a presentation by **Ilias Chantzos,** discussing the origin of cyber threats and other technical aspects. Chantzos asserted that, presently, the capabilities needed to launch a cyberattack were generally considered to be low and attackers did not need to be that sophisticated. However, he added that skilled attackers would design attacks to make identification more difficult, meaning the question of political attribution is, and will continue to be, an ongoing challenge.

Chantzos noted that these days malware could be produced on an industrial scale. Further, recorded attacks were most concentrated in countries with greater broadband internet penetration. With this exponential increase in capabilities and the proliferation of malicious activity, it is clear that there is a growing threat to the stability of the cyber domain. This reality leads to questions as to the role of well-established security firms in ensuring internet security. Chantzos asserted that the role of security companies at present was to prevent attacks, not to police the internet, which is an important distinction for the security discussion. Should there be a move towards policing the internet, it was thought likely that it would be a costly exercise more suited to governments than to corporations. Chantzos also noted that given the borderless nature of the cyber domain, mutual legal assistance regarding cyberattack would seem to depend on the willingness of states to cooperate.

The next speaker, **Larry MacFaul**, discussed the concept of verification in the cyber domain and its interaction with cybersecurity. In summary, verification was described as a way to check that states were “doing what they should be doing”, and preventing the creation or existence of an unregulated “cyber haven”. The main uses of verification are as a deterrent and as a tool to aid targeted responses to cyberattacks, he said. In his opinion, some issues for verification in the cyber domain are particularly tricky as all successful applications of verification to date have been focused on tangible things. MacFaul noted that, in theory, verification should be a very specific tool, addressing a very specific question. But in the cyber domain it is often not necessarily clear what is to be verified, therefore a broader interpretation of the concept of verification might be more useful. He posed a number of questions regarding possible verification mechanisms: Should they be national, multilateral, bilateral, multinational? Does cost–benefit analysis come into play? Will there be an asymmetrical situation where some states can verify, but others cannot? Who will carry out verification and how? Would a proposed mechanism be acceptable to those who wish to verify and those being verified?

MacFaul alluded to the difficulty of identifying perpetrators in the cyber domain, and the resultant call by some for an international body for monitoring it. He concluded, however, that this would perhaps be an overly ambitious undertaking. In the absence

of such an entity, there appears to be political support for various CBMs such as data-sharing, coordination mechanisms, joint exercises, jurisdictional agreements, and agreed enforcement action. It was also envisaged that states could possibly conduct peer review of other states' cyber legislation. MacFaul concluded that there was an appreciation that more work needed to be done to eliminate safe havens, share best practices, and create mechanisms for de-escalation, the harmonizing of legislation, and capacity-building.

The final speaker on the panel, **Ben Baseley-Walker**, approached the discussion from a different angle; rather than focusing on problems that the cyber domain posed for enforcing regulations, he highlighted the solutions offered by CBMs in this environment. He agreed that political attribution was a major hurdle to progress, but asked whether attribution should be the most important focus of ongoing discussions. He touched upon the fact that there were several significant bodies of law and enforcement mechanisms already in existence that may be applied to the cyber domain and, as a complementary addition to those mechanisms, CBMs offer an attractive way of increasing trust and transparency, while also de-emphasizing the problem of attribution that has dogged other legal instruments.

It was reiterated that several types of cyber actions have non-cyber components, and because cyber events could be seen as a potential trigger for conflict, maximizing stability and the benefit of the cyber domain was a shared goal. Baseley-Walker suggested focusing on how to establish the basis of strategic dialogue, understanding the positions of adversaries and allies, understanding deliberate actions of an offensive nature and potential responses to actions that were not intended as deliberate offensive action. He asserted that, at the multilateral level, there needs to be a better understanding of how to break down the cyber issue and where this should be done—it was not obvious at this point whether cybersecurity should come under the umbrella of the Conference on Disarmament, or if it should be addressed within the United Nations General Assembly—if the latter, there would need to be a decision on which committee. Baseley-Walker summed up by underlining that everyone has a stake in cybersecurity. It is not an issue confined to the superpowers, but is a highly globalized field with profound implications for international security. Efforts must therefore include all actors.

Panel 3
Cyber CBMs in the context of international multilateral initiatives in the cyber domain

The third panel provided an insight into current initiatives and ongoing fora on cybersecurity. The first speaker, **Neno Malisevic,** provided an overview of the work of the Organization for Security and Co-operation in Europe (OSCE) on cyber CBMs. He stressed that all stakeholders are connected by the cyber domain; therefore, it is crucial to engage threats together, irrespective of nationalities or boundaries. He indicated that the OSCE was presently organizing an informal working group tasked with drawing up a set of CBMs that might be implementable in the cyber domain. While avoiding specifics, Malisevic did reveal that the early trend is towards transparency measures.

Malisevic indicated that the range of proposed CBMs being considered by the OSCE is very broad, and that there is not unanimous agreement among member states. Nonetheless, the discussions in themselves provide an excellent foundation for further negotiations.

Where the initiative will go from here was said to be dependent on the engagement of participating states at the OSCE Ministerial Council due to take place in December 2012. Overall, it was suggested that there is a sense of optimism that some agreement could be made. It was asserted that even agreement on very low-level, common measures would represent a big step forward for multilateral cooperation in the cyber domain.

Following the OSCE overview, **Eneken Tikk-Ringas** presented on the Tallinn Manual on the International Law Applicable to Cyber Warfare and its relationship to cyber CBMs. She began by noting that CBMs have not traditionally been included in standard IHL conceptual thinking or in the law of armed conflict, but that CBMs could quite possibly be used to reinforce and strengthen international law. While Tikk-Ringas acknowledged that CBMs have the potential to aid the development and generation of new law, developing viable CBMs would require accompanying foundational or interpretational legal policy and technical analysis.

Looking at the current legal landscape, Tikk-Ringas judged that international law on criminal cooperation, telecommunications, and human rights would need further expansion and restatement if it were to be used for the purposes of cybersecurity. She pointed out this might take years of work, and restatements would need continuous follow-up and analysis of the legal relationships.

It was cautioned that it is important to bear in mind that any cyber CBMs would need to have regard for existing legal instruments and their implementation in practice—and that it was worth being mindful not to devaluate existing norms. It was underlined that CBMs may define how we interpret or understand law by creating perceptions of what constitutes the legal duty of a state—for example, cooperation in mitigation, exchange of information, and transparency of doctrine and strategy. As possible next steps, Tikk-Ringas suggested three key avenues of further work—first, development of selected CBMs to support legal responses, including criminalization of certain offences; second, legal analysis of proposed CBMs in the light of existing international instruments and norms; and third, analysis of the Tallinn Manual from a policy and technical feasibility perspective.

In the final presentation of the panel, **Kwon Haeryong** summarized the ASEAN Regional Forum (ARF) perspective on CBMs and future work on cybersecurity to be undertaken in that context. The ARF has to date carried out eight seminars and workshops on cyberspace since 2004, including a recent seminar on 11–12 September 2012 in Seoul specifically on CBMs. The Seoul seminar concluded that, in terms of CBMs, there is a need to focus on practical measures such as information-sharing, establishing a network among policy points-of-contact, and capacity-building for developing countries. Furthermore, it was noted that ASEAN states shared the view that regional CBMs should take into consideration regional characteristics. There is a strong desire within much of the ARF to establish acceptable norms of state behaviour in cyberspace, whether that be through a new code of conduct in the United Nations framework or the extension of international law to cyberspace.

The Ambassador noted that ASEAN states remained “rather unengaged in the political and military aspects of cybersecurity”. In contrast, one area where there is keen interest in the ASEAN region is in capacity-building and technical cooperation within the ARF framework.

To conclude, details were shared on the upcoming ARF conference on cyberspace which will take place in Seoul on 17–18 October 2013. This upcoming conference will feature cyberspace in the context of international security as a main topic, and will aim for a wider participation of countries.

Panel 4
Business and civil society

The final panel of the first day of CS12 showcased speakers from the private sector and civil society and provided an additional dimension to the governmental focus of the previous panels. The first panellist, **Jan Neutze**, provided a look into effective engagement between industry and the diplomatic community. While acknowledging proposals for transparency, confidence-building, and stability measures that have been put forward in other fora, he urged that these should not be implemented sequentially, but instead as a concerted effort. It was seen that governments play three distinct roles in cyberspace—as users concerned by stability and security of their systems, as protectors of the internet through incentives and regulation, and finally as exploiters of the internet seeking competitive advantage, including military advantage. Neutze called for a shift from a reactive to a more proactive approach, focusing attention on prevention. There was seen to be both a technical and political aspect to cybersecurity, and that industry could provide valuable input to both sectors. As an example, industry was described as having already established frameworks and mechanisms for information-sharing among ICT companies—frameworks that could be used as a basis for governmental sharing of sensitive data on cybersecurity.

One warning made by Neutze during his presentation was that while there may be a perception that the private sector could handle stability issues within the cyber domain, large-scale dormant capacity to deal with systemic stability issues or an onslaught of sophisticated attacks was not likely to be found anywhere in the private sector, and this left a gap that may have to be filled by governments. Neutze said the private sector planned and executed strategies for high-probability, but low-to-medium impact events—whereas it must fall to governments to address low-probability, high-impact events. He closed by noting that cybersecurity is an intrinsic part of national security, and therefore called for closer public–private partnerships and the ability for the public and private sectors to have greater interaction in international fora.

The next speaker, **Greg Austin**, sought to explain the concept of cyber dominance, and how the possible dominance of individual states might pose a hurdle to multilateral discussions. It was suggested that the cyber domain is viewed by some states as an arena for strategic military competition, and the drive for information technology dominance could distort multilateral negotiations concerning cyberspace. Austin raised the question as to whether national sovereignty could be extended to the cyber domain, given that the rise of information technology has blurred traditional boundaries. He made a number of recommendations on how to move towards cyber stability. A notable recommendation was that states should commit to the concept of strategic cyber stability, and abandon the concept of a new global multilateral agreement. He also echoed the call for future public and private sector cooperation, as well as involvement of NGOs.

The last speaker of the day was **Li Hong**, who provided a Chinese NGO point-of-view on cyber stability. Of key concern to Li was avoiding cyber war, with prevention being the priority instead of legitimizing or regulating conflict in the domain. He expressed the hope that this could be achieved through discouraging cyber military activities (especially offensive exercises), increasing bilateral and multilateral dialogue, as well as consideration of a code of conduct, CBMs and conventions.

Li proposed that the core principles for a code of conduct or for future CBMs for cybersecurity should complement the Charter of the United Nations and international law, respect the sovereignty of states in cyberspace, and incorporate a cooperative approach to reduce mistrust and misunderstanding. His assessment was that a political declaration would be more practical at the current stage than a legal commitment.

Panel 5
Looking towards the future of cybersecurity: What would a stable cyber environment look like?

The second day's proceedings commenced with a panel on the nature of a stable cyber environment. This panel showcased a variety of positions on the future direction of cyber stability, and while there were some common parallels among speakers, key divergences were apparent. **Michele Markoff** reiterated the idea that managing cyber technology is difficult—cyber technology should continue to evolve unhindered in order to continue to provide the enormous benefits that the sector brings. However, Markoff emphasized the need to manage state behaviour with respect to miscalculation and potential triggers for warfare. She expressed the position of the United States that cyber technology could be managed by applying frameworks of pre-existing legal norms, such as the law of armed conflict, thereby safeguarding civilian populations and infrastructure. In addition, the United States believes that CBMs need to be put in place in order to at least provide an element of predictability to state use, otherwise any activity in cyberspace could cause unintended reactions, miscalculations, or misattribution.

In terms of providing a policy definition for cyber stability, Markoff suggested that we are currently faced with a situation where there is no incentive for one state to attack another. However, a technical definition of cyber stability is needed. The United States sought to make progress on that front, but has not, as yet, arrived at that definition. It has urged other states to further explore this concept as well. The United States supports calls for the establishment of a framework of interaction for cybersecurity, comprised of practical confidence and stability measures that, over time, might build on one another to provide reassurance. Among the tools to achieve these goals, transparency and cooperative measures were seen as key to reducing uncertainty surrounding state cyber activities. Lastly, the United States agrees that addressing cybersecurity is important for all, but there is a particular need for initial buy-in from the most cyber-capable states. It was stressed that if any major peer state were omitted from this, stability would not be possible.

The second speaker, **Detlev Wolter**, suggested that, from a German perspective, a stable cyber environment is characterized by no incentives to attack, coupled with disincentives to attack. Such an environment was declared to have at least three main tenets—first, fewer vulnerabilities: the asymmetric architecture of the internet is one of the key sources

of vulnerability, which it is hoped that the private sector could help improve; second, greater resilience of digital control systems for critical infrastructure; and third, a common basic understanding on acceptable state behaviour, with all practical CBMs outlined.

The main challenges include technical risks and uncertainties as the prevailing trend in cyberattack leans towards more sophisticated activities targeting high-value targets—compounded by problems of attribution and the risks of uncontrollable collateral damage. A further problem is the ambiguity over which norms and rules should apply. At present, there is not considered to be consensus in the international community as to which entities in the international system should deal with these issues. In the absence of applicable rules for responsible behaviour, there is a strong concern that misunderstandings could pose enormous risks.

The third speaker, **Amandeep Singh Gill,** laid out what a stable cyber environment should look like from the perspective of India. He began by listing three caveats. First, stability in the cyber environment should not be treated as analogous to other international security environments as this would not reflect the realities of cyber technological development. Second, there needs to be a broadening of perspectives when dealing with these technologies. Third, it is important to bring emerging stakeholders into the dialogue, and expand beyond capacity-building alone. Progressing to the key elements needed for a stable cyber environment, Gill stressed that the primary characteristic needed is that any future agreements should allow for the continued and expanding use of ICTs for social and economic transformation.

Gill went on to remark that there could be no cyber stability without bridging the political divide between key stakeholders. Growing international cooperation and swift information-sharing on malicious activities were seen as a step towards stability, and public–private partnerships were seen as necessary for future cooperation. Institutionalized international dialogue to buttress CBMs is considered critical. Gill touched briefly on the rule of law aspect, and stressed that there was a need for common understandings on the application of law to cyber activities.

As the final speaker on the panel, **Sergei Fedosov** stated that the Russian Federation believes a stable cyber environment is a component of a more generally improved security climate. Cyber stability is viewed as a matter of "great significance" and it is considered that all these matters should be dealt with through international cooperation in a climate of mutual respect for the laws and cultures of other states. To that end, states could exchange national security concepts, convey timely communication of threats, and conduct consultations on cyberspace. The harmonization of national legislation, enhanced cooperation among law enforcement agencies globally, and crucially, a universal glossary of cybersecurity terms were all stated as components of a stable cybersecurity environment.

Fedosov commented that the Russian Federation views ICTs as being in the process of gradually turning into powerful tools that could have devastating effects on infrastructure, and which could therefore be seen as taking on the characteristics of weapons. In light of this, the Russian Federation deems it especially important to draw up an international, legally binding document acknowledging and dealing with such threats. The development of legal frameworks is seen as a priority, but there is also openness to other measures such

as guidelines and memoranda of intent. Going forward, it was suggested that international organizations such as the United Nations and the International Telecommunication Union should play significant role.

Panel 6
Cyber CBMs in the military context

Louise Arimatsu sought to tackle the issues surrounding "the legal application of the prohibition of the threat or use of force in cyberspace". She began by discussing how certain vocabulary such as "cyberwarfare" is misleading, as it seemed likely that any "cyberwar" would occur as part of a kinetic war, with the cyber domain merely another battlespace. Confining the discussion to state-on-state activities, Article 2(4) of the Charter of the United Nations, which states, "All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations", was considered in the context of the threshold for the use of force.

Arimatsu surmised that there were a number of factors a state was likely to consider when assessing cyber operations, such as severity of attack, immediacy, directness, invasiveness, measurability of effects, presumptive legality, and state involvement. The most significant of these aspects was judged to be the severity of attack—a cyber operation resulting in damage, destruction, or significant injury would more likely be considered a use of force than an operation resulting in mere inconvenience, but there is not a clear boundary. Among the other considerations, the level of state involvement has some interesting implications—particularly because the prohibition on the use of force might not apply if a cyber operation could not be attributed to a state. Given the well-discussed issues with attribution in the cyber domain, this was indeed an important point to note.

The next presentation was given by **Matthias Mielimonka**, and offered the perspective of the German Ministry of Defence on cyber CBMs. As with other stakeholders, the impact of cybersecurity for the military domain is significant. It follows that defence policy needs to therefore address and prioritize the increasing challenges that exist in the cyber domain. It was asserted that in spite of the rising levels of cybercrime and the potential for both industrial and political espionage, there has not yet been anything resembling a "cyberwar", and from the standpoint of the Ministry, it is doubtful that one would come about in the foreseeable future. This judgment is based on the assessment that no evidence currently exists of a cyberattack causing loss of human life, and the belief that in spite of the difficulties defining "war", all cyberattacks thus far that have disrupted infrastructure would fall far short of any proposed definition of war. In the view of the Ministry, the term cyberwar suggests a comprehensive, existential threat to a state exclusively through measures in cyberspace—and it is not thought that the cyber domain is likely to ever become an exclusive theatre of a conflict.

Mielimonka asked whether there was a difference between the cyber domain and other domains of warfare, and what were the implications for military responses to a cyberattack. It was interesting to consider, he said, whether a cyberattack would only be answered with a counter cyberattack when "an air strike … does not necessarily have to be answered with a counter air strike".

Roger Hurwitz concluded the panel with a presentation on cross-domain threat assessment in international security. He outlined that calls for the discussion of cyber norms and CBMs were motivated by escalating conflict in the cyber domain and concern about spill-over into kinetic domains. Hurwitz stated that if a cyberattack only caused disruption, there would be either no overt reaction, or just a rhetorical response. However, if damage were involved, significant cyber or even kinetic responses should be anticipated. That being said, he saw it likely that damaging cyberattacks would mostly occur in a context of pre-existing conflict or competition.

In his view, the demilitarization of cyberspace was not feasible as the "genie is already out of the bottle", and a cyber treaty would be both too complex and not dynamic enough to adapt to the changing cyber environment. Instead, he suggested a move towards CBMs, such as creating a common vocabulary and grading system of threats, developing or exploiting existing fora for handling non-military conflicts in the cyber domain, and building programmes of cyber cooperation that were both multi-stakeholder and technologically informed.

Panel 7
CBMs—what's next?

The last panel of CS12 took a forward-looking approach to cyber CBMs, focusing on directions for future development. **John Sheldon** offered an overview of data-sharing concepts, looking both at the pros and cons of this type of CBM. He noted that the benefits of data-sharing are well-documented and included increased security, mutual awareness, establishment and reinforcement of norms, and potential deterrence. However, Sheldon went on to highlight some of the limitations and drawbacks to this type of measure. For one, the costs of sharing could outweigh the benefits, as some might seek to take advantage of transparency. While it was seen as inevitable that cyberspace would always be a realm for state, organizational, and commercial competition, technical information-sharing was seen as possible without being encumbered by political issues.

Dave Clemente discussed the building of coherence and understanding in the cyber domain. He commented on how society might manage its growing dependence on cyberspace, beyond simply conceding that society is already inexorably dependent on the domain for critical infrastructure. Looking ahead to the future, Clemente supported the creation of de-escalation mechanisms and also the cyber equivalent of the Hippocratic Oath—"first do no harm". Assuming that the dynamic evolution of the cyber domain continues, it was asserted that building confidence in the cyber domain would not get easier or cheaper—thus paying for mechanisms and safeguards now might be preferable to paying in a decade.

Wrapping up the conference, **Eduardo Gelbstein** covered the role of developing countries in cybersecurity, with a particular focus on capacity-building. He outlined that capacity-building is a critical requirement for long-term stability and cyber governance, and that capacity-building was particularly essential for developing countries. The core components of capacity-building were seen to be training and motivating good security governance, and demonstrating due diligence. Contrary to earlier views, Gelbstein expressed some concern about the practical realities of information-sharing as a workable solution for the

cyber domain due to perceived bureaucracy inherent in public sector organizations, which would erode timeliness and effectiveness.

Section II

Overview of outcomes

From the outset, one of the intended goals of CS12 was to hold an event focused on cyber stability that raised the profile of such discussions with an international security community that has more exposure than most to other issues that impact on cyber stability. The CS12 conference was seen as a timely opportunity to tackle some of the current issues and challenges facing stakeholders and policymakers, and successfully brought together some 120 participants from diverse backgrounds. Given UNIDIR's mission to act as a bridge between stakeholders, it was encouraging to see the breadth and depth of participation from states, as well as the private sector, academia, and non-governmental organizations.

The presentations covered a great deal of the key substantive issues at play, including a review of ongoing processes and initiatives. A common message during the presentations and floor discussions was the need for pragmatic action going forward, beyond questions of rhetoric.

Even though the cyber domain is a multi-stakeholder environment, it is clear that, at present, many discussions concerning cyber stability and security take place in fora that only tend to cater to distinct blocs as opposed to facilitating dialogue between groups that have different equities in the cyber domain. CS12 therefore aimed to provide a unique opportunity for dialogue between specific stakeholders that do not often participate in common fora. The resultant discussions provided valuable new insights to the policy debate.

Cyber policy lagging behind advances in technology

One observation made repeatedly throughout CS12 was that the cyber domain possessed unique characteristics and posed challenges distinct from those found in other domains or when confronting other emerging technologies. The well-established rules of engagement applied to more traditional international security issues are arguably insufficient or, in some cases, unworkable, given the idiosyncrasies of the domain. Furthermore, some of the most beneficial aspects of the technology were seen as incredibly problematic from a policy standpoint. For example, cyber domain innovation and expansion proceeds rapidly without necessarily having sufficient oversight in parallel with its growth. There is a clear sense that public policy lags behind advances in technology. Discussions on the best means of regulation were considered a high priority, and the conference brought forward diverse opinions on possible solutions and what they might be.

Further complicating predictable interaction in the cyber domain is the fact that it does not conform to traditional national or legal boundaries; as such, existing laws, controls, safeguards, and conventions are somewhat limited or are not adequately tailored to dealing with the technology and its uses. Without adequate or effective regulation or

measures to discourage negative activity, the domain will be vulnerable to instability in the future.

The question was raised of how policymakers should approach cyber technology and current and potential future use. Curtailing freedom was seen as undesirable, if not impossible; but to protect the utility of this resource, there was seen to be an urgent need to discuss mechanisms for engagement, as well as tools and frameworks that might ensure the continued stability, security, and reliability of the cyber domain.

Problems of attribution, intent, and verification

A number of participants noted that the evolution of cyber technology and its integration into everyday life means that security incidents in the virtual world could increasingly have tangible impacts on the physical world. Unlike conventional security threats and attacks, a cyberattack has the possibility to be carried out with a high degree of anonymity. Countless examples of misuse of the cyber domain and attacks on a range of targets by non-state actors were alluded to during the conference presentations, ranging from actors exploiting vulnerabilities for profit, “hacktivism”, and the use of cyber resources for terrorist purposes. It was discussed that, as the cyber domain persists and expands as an integral part of numerous critical systems and infrastructures, there is clear potential for attacks on these systems by both state and non-state actors. One of the shared concerns raised by speakers and participants during the conference was that, should the cyber domain become a domain for state conflict, the consequences for all users—not only parties to the conflict—could be devastating.

The most widely cited hurdles to progress in developing international norms and policies in the cyber domain were the issues of attribution, intent, and verification. As mentioned above, the anonymity provided by cybertechnology is considered problematic from the point of view of a state with legitimate security concerns trying to understand what activities another state might be undertaking in the domain, or that might be responsible for an observed attack. Additionally, even if specific legally binding norms were in place to curtail undesirable behaviour by states in the cyber domain, it is generally considered very difficult to monitor or confirm that such norms are being adhered to—especially given that states are not the only, or even primary, actors.

When studying traditional kinetic threats and attacks, identifying the source of an attack is likely to be simpler and, to a degree, it is possible to have an overall picture of the military activities of a state. For example, a missile launched from a particular base or warship offers a very clear indication of who the attacker is—but a cyberattack may not be traceable. Even if an IP address can eventually be determined, it is still very difficult if not impossible to attribute with certainty whether an attack originating from one country is actually being instigated by that state, a proxy of another state, or a non-state actor. Indeed it was considered likely that any state-on-state attack is likely to involve a proxy in order to maintain an element of plausible deniability and uncertainty as to attribution.

There is a possibility that a cyberattack could trigger retaliatory action outside of the cyber domain. Given the difficulty of attribution, such actions may not necessarily be directed towards the true aggressor. Against a backdrop of strained international relations, such a situation could be a dangerous catalyst for war.

The lack of observable factors for identifying offensive cyber tools and the difficulty of analysing cyber activity can be seen as a hindrance to a state's ability to evaluate the capabilities of other states. It was noted that while it may be possible to measure more physical weapons through counting stockpiles, or gauging available technology and facilities, building a practical understanding of a state's cyber capabilities is far more difficult, perhaps impossible. For example a highly sophisticated and precisely engineered piece of code, such as "Stuxnet", may have a profound impact on an exact target. But far more crude viruses or low-tech denial-of-service attacks could just as easily bring about a massive disruption or loss of service with widespread consequences.

Thus the cyber domain, while undeniably beneficial in a number of regards, presents an arena of potentially heightened levels of mistrust, misunderstanding, and potential conflict.

The focus on CBMs in the cyber domain

The complexities of applying international law to cyber activities has increased consideration of the role that CBMs might play in assuring the stability and utility of the cyber environment. The essence of CBMs is that, in all interactions, intentions are correctly interpreted, messages are correctly understood, and misunderstandings do not lead to undesirable consequences.

Ambassador **Juan José Gómez Camacho** noted that one of the most challenging and pressing hurdles to ongoing diplomatic progress was the profound lack of confidence among cyber actors. Given that independent verification is difficult, states are highly dependent on others' statements regarding their intentions and capabilities. As such, increasing transparency and creating channels through which information could be shared—and misunderstandings resolved—should be key ambitions that might be achieved by the adoption of CBMs in the cyber domain.

Devising and implementing such CBMs, however, were not seen as simple endeavours. A repeated concern was that even though CBMs have been put to use in other areas of international security with varying degrees of success, the unique character of the domain requires governments to design measures specifically for it. Information technology is not exclusive to states or individuals, and therefore there is a need to be extremely careful, thoughtful, and deliberate when designing cyber CBMs in order to manage, as much as possible, unintended consequences and outcomes.

Overall, while all participants of CS12 hoped to ensure that the beneficial aspects of the cyber domain would not be curtailed, it was clear that much, if not all, of the technology was intrinsically dual-use. It is critical that dual-use technologies be controlled, and used in a responsible way. To this end, CBMs have promising potential in the cyber domain to improve the overall security climate, and speakers welcomed the opportunity to discuss and share ideas on what cyber CBMs might look like.

Legal applications and regulation

In addition to the emphasis on CBMs, there was also considerable discussion of the legal landscape and its relationship to the cyber domain. In this area of discussion, the diversity of views was great. Some saw much value in extending existing legal frameworks, while

others felt that the challenges of developing binding law in the cyber domain were a strong argument in favour of pursuing CBMs. Other participants were keen for further discussions on a possible code of conduct, without necessarily calling for a draft text at the present time. Many norms applied in other security situations, such as “no first use”, were deemed ineffective in the cyber domain, since the challenge of identifying perpetrators and the use of proxy actors would allow governments to maintain a level of plausible deniability that would render law impotent.

As regards specific bodies of law, for some participants there was a clear sense of the applicability of the law of armed conflict to state-on-state behaviour in cyberspace. Other participants supported the applicability of international law, while ruling out international humanitarian law, specifically, as to acknowledge the applicability of it to cyberspace would countenance the use of force in the cyber domain. However, this view was balanced by other assessments that civilian hackers and organized criminals had adapted information technology into attack tools prior to any systematic development by governments.

In sum, there was general consensus that existing law governing international security does not fit well with the nature of cyber technology, and much more discussion and convergence are needed on interpretations and definitions.

Concluding thoughts

UNIDIR’s 2012 Cyber Security Conference was perhaps the first event of its kind to bring together a diverse group of experienced security diplomats to discuss the international security implications of and threats to cyber stability. With the development of the internet as a global infrastructure for business and as a new tool for politics, espionage, and military activities, there is clearly growing international concern regarding the long-term sustainability and utility of cyber activities. The cybersecurity concept is still in its infancy and, as of yet, there is no multilateral venue or forum where states and non-state actors can discuss how to proceed. As this conference highlighted, given the well-known technical difficulty in attributing cyberattacks, the “rush to weaponize” the cyber domain threatens to lead to geostrategic instability and raises the potential for miscalculations in times of crisis to lead to conflict.

As cyber capabilities continue to grow and with many more states expressing interest in developing cyberdefence skills, there is a growing need to develop mechanisms for discussion, education, and constructive engagement on how to improve cybersecurity in the multilateral environment. While it is true that states need to seriously address the daunting challenges of protecting their information networks, especially those related to national security, from attack, understanding the actions of potential adversaries, communicating national redlines, and building on areas of common agreement are crucial.

The tight focus of the Conference and the high calibre of discussion on questions such as the attribution of cyberattacks, the application of international humanitarian law to the cyber domain, private industry participation in the multilateral development of cybersecurity norms, and what exactly amounts to an armed attack in the cyber domain, all laid down a strong basis for future UNIDIR discussions on cyber stability and were an

effective contribution to the difficult ongoing conversations on the future of one of the world's newest and fastest growing critical resources.

UNIDIR RESOURCES

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 this document are the sole responsibility of the author.

They do not necessarily reflect the views or opinions of the United Nations or of UNIDIR's sponsors.

This project was funded by the Governments of the Federal Republic of Germany and the United States of America.

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 the 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's activities are funded by contributions from governments and donor foundations.

Learn more at www.unidir.org.