ICT for peace FOUNDATION

CYBER POLICY PROCESS BRIEF

AMBASSADOR (RET.) **DANIEL STAUFFACHER,** EDITOR
CAMINO KAVANAGH, RAPPORTEUR

CONFIDENCE BUILDING MEASURES AND INTERNATIONAL CYBER SECURITY

GENEVA 2013
ICT4PEACE FOUNDATION

Daniel Stauffacher, Camino Kavanagh (2013) Confidence Building Measures and International Cybersecurity
ICT4Peace Publishing, Geneva.

Copies available from www.ict4peace.org

CONFIDENCE BUILDING MEASURES AND INTERNATIONAL CYBER SECURITY

Zurich, 20 and 21 June 2013 ETH ZURICH

BACKGROUND

The meeting in Zurich took place at an important moment. Recent events have shown that much remains to be done to ensure and strengthen confidence between states and society around the different uses of cyberspace. Meanwhile, mistrust between states regarding the use of cyberspace continues to rise, not least due to the increasing sophistication of cyber probes and attacks and a palpable race to enhance offensive as well as defensive capabilities.

Notwithstanding, a UN process on Developments in the Field of Information and Telecommunications in the context of international security initiated in 1998 within the framework of the UN General Assembly First Committee on Disarmament just recently reached agreement on a range of measures aimed at building cooperation for a peaceful, secure, resilient and open ICT environment. Progress is also being made within the framework of the OSCE to reach agreement on a complimentary range of CBMs and recent constructive discussions have led to a sense of cautious optimism that participating states may adopt a first set of cyber/ICT security-related CBMs at some point in 2013. Meanwhile, discussions on CBMs within the framework of the ASEAN Regional Framework (ARF) continue. At the bi-lateral level, the U.S.- Russian strategic dialogue has been long standing and has recently resulted in an agreement on some initial CBMs. The U.S.-China consultations on international cyber security are much more recent and there are indications that discussions are moving forward in a positive direction. Similar official consultations on cyber security issues are emerging in bilateral talks between other states interested in this subject matter. In addition to these developments, the government of South Korea is now preparing for the next international conference on cyberspace, which will build on the earlier efforts of the United Kingdom and Hungary to broaden the dialogue beyond state actors, and assess progress to date.

These are all important steps since earlier efforts to reach common ground on how to respond to threats to international cyber security yielded limited results, and there was an underlying perception that ideological differences in particular between blocks of states were serving as important stumbling blocks to reaching even minor agreement on norms and confidence building measures for responding to international cyber security challenges. Each of these processes has also broadened awareness on the issues, although questions regarding how to effectively engage (directly or indirectly) non-governmental organizations and the private sector remain unresolved.

WHY CBMS?

The objective of confidence and transparency building measures in recent history and in relation to conventional threats has been to prevent outbreak of war and escalation in a crisis; increase trust so as to avoid escalation; enhance early warning and predictability; and modify and transform or improve relations between states. There is general agreement that CBMs for responding to international cybersecurity issues are useful and necessary, that they are timely and that they should be a priority area for the international community. CBMs are the type of measures that need to be in place to avoid potential misunderstanding and escalation when relations among states with regard to cyber/ICT security worsen, serving as a form of pressure valve.

Regarding cyberspace, a series of cyber security challenges has emerged over time. These include:

- Low entry barriers to cyberspace, meaning that

more and more actors have access to information technology and software that can be potentially used for malicious and hostile activities.

- The fact that in highly connected societies the disruption of services can cause significant economic, financial and psychological damage thus rendering these services strategic targets.
- A growing digital divide between high-industrialized and less-developed countries and growing concerns regarding information superiority.
- Growing concerns that cyberspace is becoming militarized and that states are investing in developing offensive military capabilities aimed at destroying, denying, degrading or disrupting a perceived adversary's capabilities.
- Concerns that 'disruptive cyber tools' or 'cyber weapons' are proliferating, provoking a digital arms race and representing a new tool of warfare.
- Lack of clarity about which situations and under what circumstances 'cyber weapons' will be used.
- Increasing anxiety that civilian infrastructure will be attacked by state or non-state actors and whether such an attack would lead to escalation and the outbreak of conventional conflict.
- Increasing concern about cyber espionage, unfettered data collection, privacy and broader civil rights.

These challenges are being discussed against the backdrop of significant events in cyberspace. Both China and the United States have accused each other of conducting protracted cyber espionage activities, and more recently it has been alleged that the UK has also been involved in similar activities. It has also been revealed that the U.S. has a developed policy - and most likely doctrine - for offensive cyber operations, although it is more than likely that the U.S. is not the only country that has developed these capabilities. These revelations have had the combined counter-intuitive effect of creating a form of 'strategic pause' among the great powers, at least. There are signs that the U.S. and Russia have started a serious dialogue on international cyber security issues, and that both the U.S. and China are seriously considering similar discussions. These are positive developments that provide a degree of optimism that strategic restraint will become the rule rather than the exception in matters of offensive cyber operations, even if cyber- espionage will undoubtedly continue unabated.

Confidence building measures can serve to lay the foundation for agreeing on acceptable norms of behaviour for states as well as confidence and trust building measures to avoid miscalculation and escalation. They can also represent initial steps towards discussions on arms control and finding common ground for understanding future cyber threats in a crisis or war-like situation, including protection of strategic assets and critical civilian infrastructure. It is however, equally important to be clear about what it is we are trying to prevent, or at least mitigate when discussing different types of measures. In this regard, measures that instil strategic restraint in offensive cyber operations that have the potential of creating physical damage and harm should be the main priority. CBMs should serve that end. We should not however, delude ourselves that states will give up certain cybersecurity programs – including seemingly aggressive ones - even if processes of political and strategic reconciliation are underway. Indeed, there are shared and agreed monitoring, compliance, and transparency measures for CBM's, but realism dictates that we must also accept that states will also maintain and use private and covert measures for monitoring each other's activities and capabilities. The axiom 'trust, but verify' remains crucial in this regard.

Finally, the role of regional security organizations (RSOs) such as ARF, OSCE, OAS, AU is also crucial in helping to broker common approaches to defining CBMs and there are obvious economies of scope and scale in capitalizing on their experiences in more conventional arms areas. There has also been talk of using existing communications mechanisms in RSOs to help de-escalate tensions. Provided they work at net speed, the latter could be a useful way forward. However, the role of RSOs should be seen in its proper context: whereas CBMs on conventional forces have stressed the regional basis for CBMs, the

global interconnected nature of cyber space means that regional approaches can take us only so far. Enhanced mechanisms for sharing of good practice between and among RSOs would be a powerful step to take forward. A first step in this regard would be to institutionalize dialogue among the RSOs. In the same vein, RSO involvement should be seen as complimentary to bilateral CBMs, such as those recently announced between Russia and the US. This is a complicated problem, and a "one size fits all" solution will not work. Much of the debate so far, whether about norms or CBMs, has been about the development of consensual approaches to the issue; but it is important to bear in mind the role that declaratory policy can also play. In this regard, it is worth recalling that in conventional domains, confidence building often begins with a unilateral concession by one or more parties: in Northern Ireland, the Middle East, and the Soviet Union, for example. Declaratory policy needs to be credible, but it is often the symbolism that is important, and it does not necessarily mean giving away your most valuable bargaining chips. For example, what signal would it send if a nation – or a group of nations – were to publicly declare that should an armed conflict arise, any form of cyber offensive would be conducted in accordance with the Laws of Armed Conflict (LOAC) and principles of necessity, proportionality and distinction.

Today however, some states believe that if cyberspace is viewed as a strategic domain and the applicability of the LOAC to cyberspace is discussed, the latter will propel an arms race. Meanwhile, other states feel that clarity and observance of international law is vital, as the absence of clarity could in itself lead to misperceptions over the intent of a state, spurring a cyber arms race. States might also make a declaratory statement about how they would view and react to pre-positioning of offensive cyber capabilities on elements of their critical national infrastructure (CNI). Consensus on this topic will be difficult to achieve. Conversely, given that many nations would honour their international obligations in all domains in the event of an armed conflict, it remains unclear whether a declaratory policy or "unilateral concession" it is unclear whether this would be a helpful means to increase confidence.

The meeting in Zurich brought together a small group of experts and practitioners to discuss different types of confidence building measures, how they have been introduced into the different diplomatic processes underway, as well as prospects for their effective implementation as these processes move forward. It allowed for a focused examination and development of a list of specific, concrete and practical CBMs and an assessment of their utility and feasibility from an international security, operational and diplomatic perspective (see Annex 1 Options for Cybersecurity CBMs). The following sections provide an overview of some of these CBMs. The accompanying matrix lists these measures, highlighting those that are already being discussed within the on-going diplomatic processes noted above.

The report is divided into four main sections: i) Transparency, Compliance and Verification Measures; ii) Cooperative Measures; iii) Collaboration and Communication Mechanisms; and iv) Stability and Restraint Measures. A final section discusses next steps for diplomatic CBM processes. While the aim was to set out four categories of CBMs on the basis of function, as is evident in the report, one measure can serve more than one purpose, hence there is significant overlap between measures.

The ICT4Peace Foundation would like to thank Barbara Weekes for preparing the workshop as well as Paul Meyer and Eneken Tikk-Ringas for their support, and thank Camino Kavanagh for drafting the workshop report. Finally, ICT4Peace expresses its deep appreciation to the Swiss Federal Department of Foreign Affairs, the Schwyzer-Stiftung and the Swiss Federal Institute of Technology - ETH in Zurich for their precious support for the organization of the workshop and preparation of its reports.

Daniel Stauffacher
President
ICT4Peace Foundation
www.ict4peace.org
Zurich, June 2013

I. TRANSPARENCY MEASURES, INDICATORS OF COMPLIANACE AND MONITORING MEASURES

CBMs can serve as a stepping-stone towards more formal legally binding agreements between states. The main objectives of transparency measures within this process are to improve stability and predictability. The latter are generally tied together through two mechanisms: observation and verification. For transparency measures to work it is important to: i) develop trust; ii) decide whether to include legal dimensions; and iii) use regional organizations as a repository of nation-state views.

Given low levels of transparency, predictability and confidence over state actions, initial steps could include an agreement whereby each country establishes a baseline set of transparency measures, including for example:

- A publicly available cybersecurity strategy, complete with aims, intentions, internal structures, and budgetary allocations.
- A declared military doctrine, including command/control structures, on the use of cyber tools in times of conflict.
- Publicizing a CERT's organizational structure and contact info.
- Updated points of contact for routine and urgent contacts at operational and political levels.

The latter could be bolstered with workshops and seminars as well as enhanced sharing of information on security incidents for early-warning purposes. Establishing this baseline of measures could also be a topic for capacity building initiatives as there is already plenty of good practice to build on. Such initial steps could eventually lead to an agreement on observation and verification mechanisms and ultimately, agreed voluntary restraint measures. Indeed, what start off as essentially voluntary politically binding CBMs can change over time, eventually becoming legally binding. In the cybersecurity field states are far from this goal. However, initial steps are being taken and should be leveraged to move forward.

MONITORING AND VERIFICATION AND INDICATORS OF COMPLIANCE FOR TRANSPARENCY MEASURES

Discussions between workshop participants laid bear how difficult monitoring measures would be to implement in practice. CBMs are voluntary arrangements between state parties and are therefore politically sensitive. At a superficial level it is a simple task to determine which countries have strategies, doctrines, CERTs etc., but it is difficult to determine whether the latter are just a smokescreen, designed to hide rather than clarify true intent. In addition, compliance strays perilously close to verification. Indicators of compliance for cybersecurity CBMs must not only bear the weight of the art of the possible (which is not very much), but must also bear the weight of what is politically acceptable by all state parties concerned. The process leading to the selection of a person, organization or institution to evaluate compliance can also be complex and politically sensitive and thus requires serious discussion.

As in other areas, technological solutions are necessary, but are by no means sufficient for ensuring compliance. Given the nontrivial challenges of identifying new malware, attribution of actors and motives, and characterization of attack versus mere snooping, along with the ever- changing technological landscape of pliable networks and software, cheap innovation of new methods of attack, and so forth, technical compliance becomes overly complex. Despite these challenges however, indicators of compliance might consist of the identifiable absence of malicious activity against agreed target sets, such as hospitals, nuclear power plants, and other infrastructure such as air traffic control systems, banking sectors, and so on. Another possibility might be to allow outsiders 'crowd source' compliance, whereby the 'crowd' monitors activities and report transgressions. However, the latter possibility is mired in challenges. For example, if a malicious act were to occur against a proscribed

target set, the latter does not necessarily mean that the malicious act was conducted by the state party to the cyber CBMs or by another, altogether different actor. Again, the difficulties inherent in attributing attacks renders the task of assessing compliance extremely difficult.

Meanwhile, monitoring measures depend on the nature and intrusiveness of the cybersecurity CBMs under examination, and so – like indicators of compliance - must be able to bear the weight of what is technically possible and politically acceptable. Workshop participants suggested that monitoring measures could include:

- Using joint cyber forensic teams to investigate any suspicious activity, even if just to clear state party's of suspicion.
- Agreement between state parties to monitoring by a third-party organization and agreeing to submit their activities to random inspection by said organization.
- Joint monitoring and analysis of new malware and other potentially harmful capabilities.
- Establishing joint working groups on doctrines and technological developments.
- 'Crowd sourcing' monitoring to outsiders.

Despite these recommendations, participants noted that care should be made not to overburden the compliance and monitoring requirements of cybersecurity CBMs out of the legitimate concern that parties will find such measures politically unacceptable. In addition, such measures are technically challenging and inconclusive. Above all, that cybersecurity CBMs are political arrangements designed to bring about an easing of the underlying political motivations for cyber attacks against states that are party to such CBMs. Hence, emphasis should be given to transparency measures in cybersecurity CBMs rather than monitoring and compliance measures. That said, as political relations improve, and trust and confidence increase, these measures might be instituted as the relationship improves. Paradoxically, as relations improve, the need for monitoring and compliance measures recedes.

THE ROLE OF CIVIL SOCIETY AND THE PRIVATE SECTOR IN TRANSPARENCY MEASURES

Since cyberspace is a man made domain, challenges such as attribution and verification are also manmade. Although the private sector owns and operates a significant percentage of the infrastructure and services of cyberspace, including elements used by civil and military authorities, the debate so far over CBMs has been largely among states. Participants suggested that it would be important to bring private sector actors and civil society into the debate in a more structured manner. This is a long-term issue. It might be approached directly or through standards/regulatory approaches aimed at improving confidence levels over attribution, verification and so forth, or introducing standard quality systems such as kitemarking. Other processes have led to self-organization of the private sector (for example, the Space Data Association) around different challenges and in support of government-led processes. Yet others have led to a very active supportive role of civil society. Regardless of the approach of engaging the private sector and civil society, it would be important to ensure geographical representation the different actors while also bearing in mind some of the important nuances underpinning regional, national government-private sector and government-civil society relations in different settings before pushing for broad inclusion and participation.

The following is a set of specific transparency measures, indicators of compliance and monitoring measures discussed during the workshop that could be developed on both a bilateral and multilateral basis:

Specific transparency measures

1. Open ended consultations and dialogues on national policies, budgets, strategies, doctrine, and processes for offensive cyber operations.
2. Open-ended strategic dialogues that provide transparency on potential 'red lines' and the general set of circumstances under which a

party might consider conducting an offensive cyber operation.

3. Exchanges between military officers in war colleges, with an emphasis on attending unclassified cyber classes in each other's countries.
4. Dialogues that seek to establish understanding of, and perhaps even commonalities in, national lexicons and definitions of terms.
5. Agreement to provide full transparency on organizational arrangements.
6. Joint simulation exercises.
7. Joint table-top and command post exercises to provide greater transparency on command and control arrangements and crisis escalation management.
8. Joint threat assessments/threat modelling (inc. sharing methodology for threat assessments).
9. Observation exercises.
10. Third party verification exercises.
11. Exchange of good/effective practices in responding to threats to cyber/ICT security.
12. Exchange of data on malware and other malicious indicators of threats originating from either country.
13. Creation of joint cyber forensics teams, overseen by a third-party organization.
14. Exchange information on that might be misperceived as attacks and as a channel to ask about cyber incidents that raise national security concerns and appear to be emanating from the other's territory.

Possible Indicators of Compliance and Monitoring Measures

1. The identifiable absence of malicious activity against agreed target sets, such as hospitals, nuclear power plants, and other infrastructure such as air traffic control systems, banking sectors.
2. Using joint cyber forensic teams to investigate any suspicious activity, even if just to clear state party's of suspicion.
3. Agreement between state parties to monitoring by a third-party organization and agreeing to submit their activities to random inspection by said organization.
4. Joint monitoring and analysis of new malware and other potentially harmful capabilities.
5. Establishment of joint working groups on doctrines and technological developments.
6. Crowd sourcing monitoring and reporting.

II. COOPERATIVE MEASURES

Participants discussed cooperative measures through the lens of three different relationship models:

i. *Cooperation between like-minded states where there is already an established level of trust and cooperation.*

ii. *Cooperative measures between states that already have dialogue channels (e.g. US and Russia or China, UK and China) but where trust stands on rather shaky foundations.*

iii. *Cooperative scenarios with states where there are limited if any dialogue channels and no trust between parties.*

Cooperation is underpinned by the assumption that broad cyber stability (and not just the availability of the Internet) is a shared interest of all states.

i. *Cooperation between like-minded states- where there is already an established level of trust and cooperation.* Cooperation between like-minded states can focus on building "mutual aid"[1], for example, by breaking down the different technical layers and identifying entry points for cooperative measures including those

1 *"Mutual Aid" (Jonathan Zittrain, Harvard University, 2011) can include introducing resilience through mutual aid at various t*echnical layers or "mirroring as you link" options. Since some 80 percent of Web servers worldwide sold by Apache and Microsoft, implementation can be sought through the software updates of these two companies. Such companies have a long-term self-interest to participate. Website owners can opt-in. Other examples for other technical layers: mesh networking or website notification of malware infection.

aimed at responding to DDoS attacks.2 Another example of mutual aid highlighted the support that can be provided to countries when a cyber attack is taking place ('cyber refugee hosting'), although risks inherent in this option include the fact that the target can be shifted to the state or the company hosting the 'cyber refugee[2].'

ii. *Cooperative measures between states that already have dialogue channels (e.g. US and Russia or China, UK and China) but where trust stands on rather shaky foundations.* Under this category, efforts can be placed on strengthening cooperation through inclusion of third parties in CBM processes (i.e. bringing those that have been on the fringe into the discussions). It would also be important to ensure that the right people are sitting at the table and that security agencies and services do not overwhelm the discussions and create further mistrust between states and different stakeholders.

iii. *Cooperative scenarios with states where there are limited, if any dialogue channels and where there is no trust between parties.* In these situations, CBMs still can be first step to create trust where it doesn't currently exist although some participants noted that it is more likely that only a set of global norms on cyber security would serve as a starting point for cooperative and other forms of transparency building measures.

THE ROLE OF CIVIL SOCIETY AND THE PRIVATE SECTOR IN COOPERATIVE MEASURES

Discussions also addressed the potential role that non-governmental organizations can play when limited trusts persists within a state (state-society) and between states. Ensuring access to information on different processes is imperative in this regard. As in the session on transparency measures, emphasis was also placed on the role private sector actors could play in supporting and developing cooperative measures. For example, companies that have wide situational awareness could play the role of neutral party brought in to analyze technical issues. Other experiences could be gleaned from existing cooperative measures in which companies play an important role. For example, cooperative mechanisms that have been developed to deal with cybercrime, particularly with regard to Botnet take downs and collaborative mechanisms such as the Microsoft Digital Crimes Unit which brings together a global team of lawyers, investigators, technical analysts and other specialists whose mission is to make the Internet safer and more secure through strong enforcement, global partnerships, policy and technology solutions. Kaspersky is another notable example of a private company that has played an important role in identifying highly sophisticated malware and subsequently crowdsourcing the analysis of the malware. Additional cooperative measures within this kind of framework would include enhancing efforts to manage or regulate the market in Zero Day exploits; cooperating to deepen understanding of what represents a "disruptive cyber attack", the attribution problem, forensics and early warning issues.

The following is a set specific cooperative measures discussed during the workshop that could be developed on both a bilateral and multilateral basis:

Specific cooperative measures

1. Development of/exchange of lexicons/common terminology.
2. Exchange of information on organizations that have roles and responsibilities in ensuring cybersecurity, their structures and their mandate and regularly updated lists of contact persons within the organization. regularly updated lists of contact persons.
3. Exchange of information on good/effective practices in responding to cyber/ICT security incidents.

2 For example, following the July 2008 DDoS attacks, the Georgian government sought "cyber refuge", relocating the Presidential website to a US web hosting company after Georgian-born Nino Doijashvili, Tulip Systems, offered assistance. The Ministry of Foreign Affairs press dispatches moved to Google's Blogspot and its websites were mirrored at an Estonian website and the President of Poland. However, DDoS attacks also followed these relocation efforts. Other challenges inherent in this approach include questions of neutrality, government knowledge/approval.

4. Exchanges aimed at deepening understanding of what represents a "disruptive cyber attack", the attribution problem, forensics and early warning issues.
5. Development of joint/common guidelines for responding to cyber incidents.
6. Transfer of knowledge and technology for managing/responding to cyber incidents to developing countries.
7. Capacity building (on ICT use, ICT infrastructures, legal frameworks; CERTs).
8. Establishing consultative frameworks on threats to cyber/ICT security matters.
9. Exchange of information on the protection of human rights online and offline.
10. Exchanging documents/white papers on military doctrine.
11. Exchanges between defense/security research and academic institutions.
12. Joint threat assessments (including sharing methodology for threat assessments).
13. Joint simulation exercises.
14. Exchanges on intelligence regarding malware/ incidents etc. (beyond level of CERTs).
15. Joint mechanisms for crisis management (including traditional hotlines).
16. Joint exercises in incident response (e.g. along the lines of bot-net take-downs in the area of cybercrime).
17. Joint efforts to manage or regulate the black market in Zero Day exploits.
18. Joint forensic investigations.
19. Third party verification exercises.

III. COMMUNICATION AND COLLABORATIVE MECHANISMS

During this session, participants discussed the importance of identifying key mechanisms that states could use as a means to regularly communicate and consult on cyber security issues. They also discussed the type of consultative processes that would be useful for countries that remain outside the top tier on cyber security. Discussions focused predominantly on the mechanisms for sharing threat and indicator information since the latter allow for a better understanding of capabilities, and an increased awareness that attacks can have consequences for everyone.

The following is a set of specific communication and collaborative measures discussed during the workshop:

Specific communication and collaborative mechanisms

1. Regular exchanges of information at bilateral, pluri-lateral and multi-lateral levels as well as dissemination of national strategies.
2. Listening and learning from conducting field visits, participation in international fora and consultative meetings.
3. Joint assessments, shared threat assessments and joint forensic analysis.
4. Establishment of joint/common crisis management frameworks (for high security incidents i.e. beyond CERT level).
5. Communication channels in case of escalation, recognizing above all, the need for the exchange of information.
6. Shared decision-making and collaboration within international fora and standard setting organizations within which working groups include stakeholder representatives and joint committees push decision makers to collective instead of unilateral agreement.
7. Shared advocacy.

8. Shared approaches to developing statistics/ baselines, monitoring and reporting.
9. Global public consultations to allow citizens to voice their concerns make suggestions regarding the types of cybersecurity norms they would like to see in place.
10. As a means to include non-cyber 'powers' in CBM discussions that might not necessarily affect them now but might later, participants recommended inviting the latter to work with those states that already have evolved strategies on specific challenges.

Finally, participants raised the point that attempts should be made to avoid limiting measures to old work constructs and traditional approaches to security dilemmas. The establishment of hot lines – a measure adopted during the Cold War – was tabled as an example of how measures under discussion tend to fit existing constructs. It would be important to determine innovative ways for establishing communication channels between states for the purpose of crisis management. Participants also tabled the suggestion of global public consultations that would allow citizens to voice their concerns make suggestions regarding the types of cybersecurity norms they would like to see in place.

IV. STABILITY/ RESTRAINT MEASURES

After transparency, cooperation and consultations, reaching agreement on certain stability measures would be the most demanding form of collaboration among states. The latter would only be possible if a record of successful cooperation was demonstrated in the other areas. The sharing of good practices and experiences and common understanding of how to achieve shared goals would also be a necessary precursor to discussing the types of activities that threaten international cyber security and possible restraint measures. And although stability and restraint measures are usually the most demanding element of CBMs and consensus on them generally emerges towards the end of a process, some participants felt that with regard to cyber security, efforts to agree on restraint measures with a focus on seeking to establish a confidential dialogue among sophisticated cyber powers, should commence already. The role of neutral facilitators would be particularly important in this regard.

As noted in the preceding sections, cooperation is generally more feasible between allies and like-minded countries. However, participants questioned whether developments such as the deployment of capabilities such as Stuxnet, or recent revelations about covert data collection initiatives are provoking mistrust between this group, potentially requiring the introduction of restraint measures, including declaratory statements.

Discussions also focused on the importance of distinguishing between countries that might need to engage in discussions on restraint measures and those for whom the discussion might not be so relevant (reference to digital divide). For example, a first phase could focus on those states that have developed the most sophisticated cyber capabilities, with middle states entering the discussion downstream. In the meantime, and with a view to the future, certain soft elements of 'cyber' restraint can also be weaved into other policy areas, including development (post-2015 development agenda, particularly MDG 8) and broader international security issue areas.

In terms of states with advanced cyber capabilities, participants noted the importance of determining what types of behaviour to restrain. For example, the majority of attacks to date represent acts of espionage, sabotage and subversion, not acts of war. Nevertheless, the line between cyber espionage and cyber attacks is thin: if a computer can be penetrated, it can just as easily be manipulated or disrupted. In addition, despite current rhetoric, it is highly unlikely that powerful states will engage in cyber warfare in peacetime; rather as in the case of electronic warfare, cyber capabilities will be shaped to serve as a facilitator/enabler of kinetic attacks during wartime. Responses should therefore be crafted accordingly and war-related discourse around such issues avoided or toned down so as not to drive an arms race or escalation between states on issues directly or indirectly related to cyberspace

and cyber security. As in other domains, joint strategic analysis aimed at assessing capabilities (offensive and defensive capabilities), identifying interests and positions as well as understandings of differing strategic concepts and their applicability to cyberspace should be undertaken regularly as a means to identify entry points for discussing restraint measures. At the same time however, effective measures to avoid miscalculation and potential escalation should be addressed and put in place as soon as possible.

Finally, participants discussed the potential of constraining the spread of sophisticated cyber capabilities to other states and non-state actors and whether the core group that has developed such capabilities to date could take a lead in that regard. The latter might however be rebuffed by states that are interested in developing cyber capabilities and who view limited resolve by those who already have the capabilities to exercise restraint. Such a measure might also exacerbate existing tensions between major and emerging powers, developed and developing states.

The following are a set of specific stability and restraint measures, discussed during the workshop that could be introduced at both a bilateral and multilateral basis:

Specific stability and restraint measures

1. Agreement on international technical standards that raise the barriers for developing cyber capabilities and the development of tactical warning and assessment capabilities (whether an attack is likely, by whom, at what and how significant) at what).
2. Abiding by restraints inherent in international law and its core principles.
3. Agreement on distinguishing between prohibited actions that reflect compliance with international legal obligations, including international humanitarian law and additional constraints that would be a function of mutual agreement and which would be motivated by international security interests such as crisis management and strategic stability).
4. Measures to ensure continuity, security and stability of the Internet during crisis.
5. Pledges to remove incentives for first strike offensive or/retaliatory actions or for promoting the responsible use of cyber capabilities).
6. Agreement to delimit or restrict the type of systems that could be targeted as part of cyber operations (e.g. exclusion of military CII structures, critical infrastructure from target lists.
7. Agreement to restrict the nature of the cyber intrusions militaries conduct (e.g. limiting action to computer network exploitation versus computer network attack, or alternatively setting aside certain categories of military targets, like some command and control entities in order to ensure crisis communication).
8. Excluding cyber offensive operations in third party countries during crisis.
9. Establishing voluntary "communities of responsible states" that could develop active approaches to enhancing international ICT stability, including refraining from engaging in activities they agree are inherently destabilizing or by promoting practices that enhance trust and stability.
10. Agreement on measures to reduce the prospect of proxies (including individuals, groups, criminal organizations) that might engage in disruptive activities on behalf of others, including states.

V. WHAT NEXT FOR CBM PROCESSES?

As noted by participants, within the international system, states continuously have to make decisions on how best to take forward a given initiative or enterprise in response to existing or emerging challenges. The latter includes deciding on CBMs for international cyber security. Devising a substantive proposal is only part of the effort. Equally important is identifying the right fora and

processes to encourage their adoption, and ensuring effective implementation.

The international community is at an early stage in developing cyber security policy and norms for responsible state behaviour with regard to cyber space. And while the number of platforms to discuss these matters is still limited, as noted at the outset of this report, progress is being made and the overall goal remains international cooperation on cyber security. Moving forward however, it will be important to sustain and strengthen traditional modes for realizing cooperative measures amongst states, namely at the bilateral, pluri-lateral and multi-lateral levels since the latter continue to constitute the diplomatic channels most suitable to advancing CBMs.

As noted at the outset, at the *bilateral level*, dedicated cyber security dialogues on the part of leading states with cyber ambitions are already happening. These have frequently been configured as part of broader strategic consultations already established by the parties. Such consultative channels could eventually be expanded to a broader base of CBMs, and serve as review mechanisms for their implementation. Conversely, in light of the continued high degree of sensitivity surrounding cyber security, it may prove easier for the states currently involved to experiment with specific CBMs with partners with which they already have a strategic relationship or a high motivation to establish one. At the same time however, measures agreed in bilateral channels should be transparent to outside parties so as to avoid suspicions that arrangements are being concluded between states with superior cyber capabilities that may be detrimental to the interests of those with lesser capabilities.

At the *multi-lateral level* efforts via or between regional security organizations such as the OSCE, the ASEAN Regional Forum, the OAS and the AU should continue to be strengthened. As noted, important work on cyber security is already underway in some of these forums. To the extent that other regional security organizations can follow suit, increased activity on this agenda in the coming months and years can be expected. It will be necessary however for this activity to progress beyond the discussion mode to something more operational or institutional in nature.

The final and most inclusive multi-lateral forum for resolving international cyber security issues remains the United Nations. If states are to adhere to certain norms of responsible behaviour in cyber space it is obvious in the general interest for that adherence to be as universal as possible and working under the auspices of the UN can facilitate this. On the other hand, forging a consensus around specific CBMs may prove difficult given the numbers and diversity of states in the UN system, as well as existing tensions between blocks of states within the organization. As noted, some official UN action is already underway, with the important reference of the 2010 report from the UN Group of Governmental Experts on ICTs in the Context of International Security and the potentially even more important result from the current Group of Governmental Experts (GGE) which is due to report to the UN General Assembly in September 2013. Whatever the substantive outcome of the report, the issue of CBMs in the context of inter-state behaviour in cyber space is now firmly on the agenda of the UN and its First Committee in particular, and specific proposals by states are expected. Maintaining a relatively narrow and operational focus on the international security aspect of inter-state cyber cooperation will be necessary to ensure that next steps remain productive.

Finally, the key role that the private sector and civil society can and should play in these processes is worth reemphasizing. The official work of the state-centric international and regional bodies as well as bi-lateral exchanges has always been enhanced by the involvement of non-state experts via Track II dialogues, structured exchanges and the like. Civil society and the private sector should continue to serve as a testing ground for concepts and specific measures put forward by states prior to their official endorsement.

ANNEX 1

Options for Cybersecurity CBMs: ICT4Peace Foundation Workshop, Zurich, June 2013

ON-GOING PROCESSES	BI-LATERAL PROCESSES UNDERWAY	MULTILATERAL PROCESSES UNDERWAY	PLURI-LATERAL PROCESSES UNDERWAY	PRIVATE SECTOR INVOLVEMENT	ACADEMIA / RESEARCH INSTITUTIONS	CIVIL SOCIETY INVOLVEMENT
	US-RU:T 1	UN/GGE	LONDON PROCESS (+ Budapest + South Korea)	Increased involvement advocated in GGE report	Increased involvement advocated in GGE report	
	US-CH: T 1.5	OSCE				
	UK-CH: T 2	ARF				
TRANSPARENCY MEASURES						
Open ended consultations and dialogues on national policies, budgets, strategies, doctrine, and processes for offensive cyber operations.		OSCE				
Open-ended strategic dialogues that provide transparency on potential 'red lines' and the general set of circumstances under which a party might consider conducting an offensive cyber operation.		UN/ GGE				
Exchanges between military officers in war colleges, with an emphasis on attending unclassified cyber classes in each other's countries.		UN/ GGE				
Dialogues that seek to establish understanding of national lexicons and definitions of terms.		OSCE				
Agreement to provide full transparency on organizational arrangements.						
Joint simulation exercises.						
Joint table-top and command post exercises to provide greater transparency on command and control arrangements and crisis escalation management.						
Joint threat assessments/ threat modeling (inc. sharing methodology for threat assessments)						
Observation exercises.						
Third party verification exercises.	US-RU					
Exchange of good/effective practices in responding to threats to cyber/ICT security.						
Exchange of data on malware and other malicious indicators of threats originating from either country.						
Creation of joint cyber forensics teams, overseen by a third-party organization.						
Exchange information on that might be misperceived as attacks and as a channel to ask about cyber incidents that raise national security concerns and appear to be emanating from the other's territory.						

continues ...

COMPLIANCE INDICATORS & MONITORING OF TRANSPARENCY MEASURES	BI-LATERAL PROCESSES UNDERWAY	MULTILATERAL PROCESSES UNDERWAY	PLURI-LATERAL PROCESSES UNDERWAY	PRIVATE SECTOR INVOLVEMENT	ACADEMIA/ RESEARCH INSTITUTIONS	CIVIL SOCIETY INVOLVEMENT
The identifiable absence of malicious activity against agreed target sets, such as hospitals, nuclear power plants, and other infrastructure such as air traffic control systems, banking sectors.						
Crowd sourcing of activities and reporting via independent outsiders.						
Using joint cyber forensic teams to investigate any suspicious activity, even if just to clear state party's of suspicion.						
Agreement between state parties to monitoring by a third-party organization and agreeing to submit their activities to random inspection by said organization.						
Joint monitoring and analysis of new malware and other potentially harmful capabilities.						
Establishment of joint working groups on doctrines and technological developments.						
COOPERATIVE MEASURES						
Development of/exchange of lexicons/common terminology.		OSCE				
Exchange of information on organizations that have roles and responsibilities in ensuring cybersecurity, their structures and their mandate and regularly updated lists of contact persons within the organization.		OSCE				
Exchange of information on good/ effective practices in responding to cyber/ICT security incidents.		OSCE, UN/ GGE				
Exchanges aimed at deepening understanding of what represents a "disruptive cyber attack", the attribution problem, forensics and early warning issues.						
Development of joint/common guidelines for responding to cyber incidents.		GGE (in ref. to disruptions perpetrated bynon-state actors)				
Transfer of knowledge and technology for managing/responding to cyber incidents to developing countries.		UN/ GGE				
Capacity building (on ICT use, ICT infrastructures, legal frameworks; CERTs).		UN/ GGE		Yes - within framework of GGE process		
Establishing consultative frameworks on threats to cyber/ICT security matters.		OSCE				
Exchange of information on the protection of human rights online and offline.						
Exchanging documents/ white papers on military doctrine.		OSCE				
Exchanges between defense/security research and academic institutions.						
Joint threat assessments (including sharing methodology for threat assessments).						

continues ...

COMPLIANCE INDICATORS & MONITORING OF TRANSPARENCY MEASURES	BI-LATERAL PROCESSES UNDERWAY	MULTILATERAL PROCESSES UNDERWAY	PLURI-LATERAL PROCESSES UNDERWAY	PRIVATE SECTOR INVOLVEMENT	ACADEMIA/ RESEARCH INSTITUTIONS	CIVIL SOCIETY INVOLVEMENT
Joint simulation exercises.						
Exchanges on intelligence regarding malware/ incidents etc. (beyond level of CERTs).						
Joint mechanisms for crisis management (including traditional hotlines).						
Joint exercises in incident response (e.g. along the lines of bot-net take-downs in the area of cybercrime).						
Joint efforts to manage or regulate the black market in Zero Day exploits.						
Joint forensic investigations.						
Third party verification exercises.						
COMMUNICATION AND COLABORATIVE MECHANISMS						
Regular exchanges of information at bi-lateral, pluri-lateral and multi-lateral levels as well as dissemination of national strategies.						
Listening and learning from conducting field visits to participation in international forums and consultative meetings.		OSCE, UN/GGE				
Joint assessments, shared threat assessments and joint forensic analysis.						
Establishment of joint/ common crisis management frameworks (for high security incidents i.e. beyond CERT level).		OSCE, UN/GGE				
Communication channels in case of escalation, recognizing above all the need for the exchange of information.						
Shared decision-making and collaboration within the international fora and standard setting organizations within which working groups include stakeholder representatives and joint committees push decision makers to collective instead of unilateral agreement.						
Shared advocacy.						
Shared approaches to developing statistics/ baselines, monitoring and reporting.						
Global public consultations to allow citizens to voice their concerns make suggestions regarding the types of cybersecurity norms they would like to see in place.						
As a means to include non-cyber ‘powers’ in CBM discussions that might not necessarily affect them now but might later, participants recommended inviting the latter to work with those states that already have evolved strategies on specific challenges.						
RESTRAINT MEASURES						
Agreement on international technical standards that raise the barriers for developing cyber capabilities and the development of tactical warning and assessment capabilities (whether an attack is likely, by whom, at what and how significant).						
Abiding by restraints inherent in international law and its core principles.		OSCE, UN/GGE				
Agreement on distinguishing between prohibited actions that reflect compliance with international legal obligations, including international humanitarian law and additional constraints that would be a function of mutual agreement and which would be motivated by international security interests such as crisis management and strategic stability).						
Measures to ensure continuity, security and stability of the Internet.						

continues ...

RESTRAINT MEASURES	BI-LATERAL PROCESSES UNDERWAY	MULTILATERAL PROCESSES UNDERWAY	PLURI-LATERAL PROCESSES UNDERWAY	PRIVATE SECTOR INVOLVEMENT	ACADEMIA/ RESEARCH INSTITUTIONS	CIVIL SOCIETY INVOLVEMENT
Establishment of joint/ common crisis management frameworks (for high security incidents i.e. beyond CERT level).		OSCE, UN/GGE				
Pledges to to remove incentives for first strike offensive or / retaliatory actions; or for promoting the responsible use of cyber capabilities).						
Agreement to delimit or restrict the type of systems that could be targeted as part of cyber operations (e.g. to remove incentives for first strike/ retaliatory actions; or for promoting the responsible use of cyber capabilities).						
Restrict the nature of the cyber intrusions militaries conduct (e.g. limiting action to computer network exploitation versus computer network attack; or alternatively to set aside certain categories of military targets, like some command and control entities, in order to ensure crisis communication for termination of hostilities).						
Exclude cyber offensive operations in third party countries.						
Excluding cyber offensive operations in third party countries during crisis.						
Establishing voluntary “communities of responsible states” that could develop active approaches to enhancing international ICT stability including by refraining from engaging in activities they agree are inherently destabilizing or by promoting practices that enhance trust and stability.						
Agreement on measures to reduce the prospect of proxies (including individuals, groups, criminal organizations) that might engage in disruptive activities on behalf of others, including states.						

ANNEX 2

GLOBAL DIALOGUE ON CONFIDENCE BUILDING MEASURES AND INTERNATIONAL CYBER SECURITY

Zurich, 20 and 21 June 2013

ETH ZURICH

The objective of workshop is to examine specific CBMsa applicable to cyberspace and an assessment of their utility and applicability from an international security, operational and diplomatic perspective. It is hoped that the discussions will help inform future consideration of confidence building in cyberspace and related policy options.

AGENDA

WENDESDAY, 19 JUNE

19:30

Welcome Dinner

THURSDAY, 20 JUNE

08:30-09:00

Welcoming remarks and introduction and brief tour de table

09:00-10:30

The Role of Confidence Building Measures - 20 minutes

A sketch of how CBMs serve the goals of cooperative security in theory and practice. Familiarization with CBMs as they have been developed in the context of international security and in previous contexts of high levels of mistrust. What has been the historic experience in regional security? Why are CBMs still valid in the cyber context? How to ensure the involvement of the private sector as one of key enablers for CBMs?

Monitoring and Compliance - 20 minutes

Once measures have been agreed on paper, there is always the question of their implementation. How would this be best accomplished for cyber security CBMs? What are the technical capabilities for monitoring adherence to agreed measures? What provisions for clarification and consultation might be considered to support the agreed measures? Is there a role for an existing international or regional organization in supporting implementation (along the lines of the OSCE for conventional measures or

Contact Points for Codes of Conduct?) What sort of on-going reporting or periodic review of measures should be considered as part of a package of agreed CBMs?

Update: Diplomatic processes - 15 minutes

Overview and update of diplomatic processes on the status of CBMs talks to date.

Briefings will be followed by a moderated discussion for approximately 30 minutes.

10:30-11:00

Coffee Break

11:00-13:00

Transparency Measures

We already see that some things are difficult to hide, e.g. capabilities. In order to now build confidence we need to make some things transparent between stakeholders, what is the minimum required level of transparency needed from a national perspective? What impact do differing national and regional perspectives have? What can a country do to implement effective transparency measures? What would provide transparency taking into account regional interests, level of development, and advancement of information society? ? How can transparency measure be monitored/complied with?

13:00-14:30

Networking Lunch

14:30-16:30

Cooperation Measures

Some work is already taking place on a bilateral level to cooperate on certain aspects of cybersecurity. How can this type of initiative be expanded on, or replicated more broadly? What effect do differing national and regional perspectives have on the types of cooperation measures that are feasible? What would be effective cooperation measures that a national government could implement? How could cooperation measure be monitored/complied with?

16:30

Coffee Break and open discussion

FRIDAY, 21 JUNE

09:00-10:15

Communication and consultative mechanisms

This session aims to identify key mechanisms, which countries can agree on to communicate and consult regularly on cyber security issues. What kind of mechanisms need to be created and implemented that do not already exist? What kind of consultative processes would be useful for countries, in particular those outside the top tier on cyber security?

10:15-10:30

Coffee break

10:30-11:30

Restraint measures

The goal of the session will be to identify different areas, including abilities, applications, sectors, that could be subject to restraint measures and what form these measures might take. How could such measures be monitored and complied with?

11:30-12:30

Next Steps and Diplomatic Channels

What options exist to advance the measures discussed during the workshop? How can preferences for different diplomatic fora, e.g. UN or OSCE or regional forums, be managed without diluting any potential cooperation efforts/progress? How to advance improved common understanding on CBMs in the various fora on Cyber security and CBMs (UN/GGE, OSCE, ARF, London Process and 2013 Conference on Cyberspace in Seoul in October 2013)?

What role for ICT4Peace? Other organizations? Key dates?

Presentation of Seoul Conference: Concluding Remarks

GLOBAL DIALOGUE ON CONFIDENCE BUILDING MEASURES AND INTERNATIONAL CYBER SECURITY

Zurich, 20 and 21 June 2013

List of Participants

1. Minister **Michele Coduri,** Federal Department of Foreign Affairs of Switzerland
2. **Nick Haycock**, International Security Team, Office of Cyber Security and Information Assurance, Cabinet Office, UK
3. Prof. **Dirk Helbing**, Chair of Sociology, in particular of Modelling and Simulation,ETH, Zurich
4. **Marc Henauer**, Head, MELANI, Switzerland
5. **Marie Moe**, Expert, GovCERT, Norway
6. **Camino Kavanagh**, Researcher, Kings College London & Senior Fellow, NYU
7. Dr. **So-Jeong KIM**, Senior Researcher, Attached Institute of ETRI, Seoul
8. **Laura Crespo**, Federal Department of Foreign Affairs of Switzerland
9. Ambassador **Benno Laggner**, Head, Division for Security Policy and Crisis Management, Federal Department of Foreign Affairs of Switzerland
10. **Nemanja (Neno) Malisevic**, Cyber Security Officer, OSCE Secretariat, Transnational Threats Department
11. **Tim Maurer**, Program Associate, New America Foundation & Adjunct Fellow, Center for Strategic and International Studies, Washington DC
12. Ambassador **Paul Meyer**, Professor, Simon Fraser University, Canada
13. Professor **Götz Neuneck**, Stellvertretender Direktor, Institut für Friedensforschung und Sicherheitspolitik, Germany
14. Dr. **Hyung-Jun Seo**, Senior Researcher, Korea
15. **Gustaf Salomonsson**, National Defence Research Institute (FOI), Sweden
16. Dr. **John B. Sheldon**, Senior Fellow in Security Studies at the Munk School of Global Affairs, University of Toronto, Canada
17. Dr. **Chris Spirito**, International Cyber Lead, MIT Research Corp, USA
18. Dr. **Eneken Tikk-Ringas**, Senior Fellow for Cyber Security, IISS; Senior Advisor, ICT4Peace Foundation, Switzerland
19. **Barbara Weekes**, Senior Advisor, ICT4Peace Foundation, Switzerland
20. Dr. **Daniel Stauffacher**, President, ICT4Peace Foundation, Switzerland

ICT4Peace

www.ict4peace.org

ICT4Peace was launched as a result of the World Summit on the Information Society in Geneva in 2003 and aims to facilitate improved, effective and sustained communication between peoples, communities and stakeholders involved in conflict prevention, mediation and peace building through better understanding of and enhanced application of Information Communications Technology (ICT). The ICT4Peace Cyber Security Program was started in 2011. We are interested in following, supporting and leading bilateral and multilateral diplomatic, legal and policy efforts to achieve a secure, prosperous and open cyberspace. (Please find the following publications of ICT4Peace on cybersecurity and resilience under: http://ict4peace.org/?p=1076):

- Getting down to business: Realistic goals for the promotion of peace in cyber-space (2011)
- ICT4Peace brief on upcoming Government Expert consultations on Cyber-security (GGE) at the UN in New York (2012)
- An overview of global and regional processes, agendas and instruments (2013)

Camino Kavanagh

Camino Kavanagh is currently pursuing a Ph.D. at the Department of War Studies at King's College London. Her research is centered on transformation in strategic affairs, with a specific focus on how cyberspace has evolved into a domain of strategic competition between states and she engages in different initiatives and projects on this subject. Camino is also a Senior Fellow at NYU's Center on International Cooperation and currently serving as an advisor to the Kofi Annan Foundation on the evolution of organized crime and drug trafficking in West Africa. She has worked with United Nations peace operations in Guatemala and Burundi and other international organizations in Africa, Asia, and Latin America & the Caribbean. She has a MA in Contemporary War Studies and a MA in Human Rights Law.

Daniel Stauffacher

Daniel Stauffacher, a former Ambassador of Switzerland, has a Ph.D. in media and copyright law from the University of Zürich and a Master's degree in International Economic Affairs from Columbia University, New York. After working for a Swiss publishing company, he joined the UN in 1982 and worked in New York, Laos and China. Subsequently he joined the Swiss Federal Office for Foreign Economic Affairs (Bawi) in 1990, where he was a Director for Economic and Financial Co-operation with major Asian and Central and Eastern European countries. In 1995, he was posted to the Swiss Mission to the European Union in Brussels as Counsellor for Economic and Financial Affairs. In 1999, he became Ambassador of Switzerland to the United Nations in Geneva and New York and the Swiss Federal Government's Special Representative for the hosting and preparation of the United Nations World Summit for Social Development (Geneva, 2000) and of the UN World Summit on the Information Society (WSIS) that was held in Geneva in 2003 and in Tunis 2005. He was a member of UN SG Kofi Annan's UN ICT Task Force. Dr. Stauffacher is the Founder and Chairman of ICT4Peace Foundation (www.ICT4Peace.org), President of the Geneva Security Forum (www.genevasecurityforum.org). He is a founding Trustee of Tim Berners Lee's World Wide Web Foundation (www.webfoundation.org) and serves as a Special Advisor to the UN Secretariat and the Swiss Federal Department for Foreign Affairs.

ICT for peace FOUNDATION