The UN Takes a Big Step Forward on Cybersecurity

Arms Control Today

Detlev Wolter

After a year of difficult negotiations, a UN group of governmental experts on cybersecurity agreed on a substantial and forward-looking consensus report. It represents an important achievement for the maintenance of international peace and stability in this new and crucial area.

By acknowledging the full applicability of international law to state behavior in cyberspace, by extending traditional transparency and confidence-building measures, and by recommending international cooperation and capacity building to make information and communications technology (ICT) infrastructure more secure around the world, the report lays a solid foundation for states to address the mutual risks that arise from rapidly increasing cyberthreats.

For the United Nations, it was high time to act to address this new international security challenge. Increasingly, more-sophisticated cybertools allow states to attack the control systems of critical infrastructure. These tools, coupled with a widespread uncertainty about the rules that would govern state behavior in cyberspace, have raised the risk of cyberconflict between states. It was therefore of crucial importance that the UN find common ground to address these challenges by affirming and clarifying the application of international law to state behavior in cyberspace and by recommending confidence-building measures.

On June 7, the group of experts agreed on a substantial report to UN Secretary-General Ban Ki-moon. The report, publicly released August 9, is entitled “On the Developments in the Field of Information and Telecommunications in the Context of International Security.”[1] In 2012, Ban appointed the group of 15 experts from the five permanent members of the UN Security Council plus Argentina, Australia (the chair), Belarus, Canada, Egypt, Estonia, Germany, India, Indonesia, and Japan to carry out a mandate from the UN General Assembly to “study possible cooperative measures in addressing existing and potential threats” related to the use of ICTs. This mandate was more specific than those for expert groups on the topic established in 2005 and 2010, as it explicitly highlighted the need to elaborate confidence-building measures and “norms, rules or principles of responsible behaviour of States.”[2]

UN member states have contributed in varying degrees to requests by the General Assembly to report on their views on international law and cooperation to prevent destabilization of state relations in cyberspace.[3] According to a recent study by the UN Institute for Disarmament Research, more than 40 states have now developed some military cybercapabilities, 12 of them for offensive cyberwarfare.[4]

The most recently appointed group of governmental experts met for week-long sessions in New York and Geneva, in August 2012, January 2013, and June 2013. The June session coincided with important progress in bilateral U.S. negotiations with Russia and with China on cybersecurity.

At the summit of the Group of Eight industrialized countries in Northern Ireland in June, President Barack Obama and Russian President Vladimir Putin jointly announced they had finalized a first-ever bilateral agreement on confidence-building measures in the cyber domain. These measures cover information exchange and crisis communication. Three kinds of cyber-specific crisis communication channels were established: a channel between computer emergency response teams (CERTs) from the two countries to discuss malware stemming from each other’s territory, a link between nuclear
risk reductions centers for cyberincidents of national security importance, and a telephone hotline between the White House and the Kremlin for major cyberincidents.\[5\] With China, the United States was able to agree to set up a bilateral working group on cybersecurity issues to diffuse growing tensions over mutual accusations of massive cyberintrusions for purposes of military and economic intelligence.\[6\] This progress with two major adversaries in cyberspace was critical in helping to achieve a positive outcome in the experts group.

The group’s report covers four essential categories for enhancing international cybersecurity: cooperation, international law, confidence-building measures, and improvements in states’ capacities for building robust ICT infrastructures. Altogether, the report presents a coherent set of a common international approaches and specific measures to promote the peaceful use of cyberspace in the interest of preventing international conflicts.\[7\]

### Risks, Threats, Vulnerabilities

Several factors make the situation in cyberspace particularly difficult to control. In addition to the absence of a common understanding on the applicable international rules for state behavior in that domain, many of the tools in cyberspace can be used for both legitimate and malicious purposes. States and nonstate actors are carrying out increasingly sophisticated exploitations of vulnerabilities in ICT. Attribution to a specific perpetrator continues to be difficult, increasing the risk of “false flag” attacks—that is, attacks by a state, group, or individual under an assumed identity.

Global connectivity, vulnerable technologies, and anonymity facilitate the spread of disruptive cyberactivities that may cause considerable collateral damage, for example, by spreading malware into computer networks or digital control systems that were not the primary target of the original attack. The experts group report highlights the specific risks stemming from the widespread use of ICTs in critical infrastructure, particularly through so-called ICT-enabled industrial control systems such as those used in nuclear power plants and other critical infrastructure.

To address these new risks, the report calls on member states to agree on an array of international actions in the four categories to promote a “peaceful, secure, open and cooperative ICT environment.”\[8\] At the outset and as a framework for all the categories, the group recognizes the importance of participation by the private sector and civil society in these efforts.

### A Universal Legal Framework

For the first time at the UN level, a group of governmental experts was able to agree to an important set of recommendations on norms, rules, and principles of responsible behavior by states in cyberspace. Governmental experts from the five permanent members of the UN Security Council and 10 leading cyberpowers from all regions of the world have recognized that international law, including the principles of the law of state responsibility, fully apply to state behavior in cyberspace. This recognition represents a landmark step toward universal acceptance of the legal framework.

The previous lack of clarity as to what rules apply in cyberspace was one of the factors contributing to instability and the risk of escalation. The explicit affirmation that international law, particularly the principles of the UN Charter, is applicable to state activities in cyberspace, including to activities of nonstate actors attributable to states, will allow the international community and affected states to react to violations more effectively. In cyberspace, states have to comply with the prohibition on the use of force, the requirement to respect territorial sovereignty and independence, and the principle of settling disputes by peaceful means in the same way as in the physical world. The right, specified in Article 51 of the UN Charter, to self-defense including the use of force would apply if a cyberattack reached the level of an “armed attack.” The report, however, refrained from spelling out when this could be the case as the legal debate on this issue has only just begun.

These principles of universal law go beyond restricting the use of force in cyberspace. They also cover other areas such as sovereignty and territorial integrity, which restrict the lawfulness of potentially harmful acts below the level of kinetic force. In particular, together with the customary international law principles of state responsibility, the principles of the UN Charter would limit the legitimacy of state actions purposely breaching the intellectual property of companies or the
personal data of individuals. Nevertheless, legal experts need to do much more work to specify these principles and rules to cover more specifically a range of diverse actions in cyberspace. Attribution continues to be a key challenge, as legal and technical attribution are required in order to challenge a state, for example, in the Security Council, for wrongful acts in cyberspace.\[9\]

Concerning cyberattacks that reach the threshold of an armed conflict, a lower threshold than armed attack, most of the 15 experts were willing to explicitly acknowledge the application of international humanitarian law to cyberspace.

Russia has accepted the application of such law to cyberspace. China, on the other hand, has repeatedly stated that it considers such explicit confirmation premature and counter to the objective of preventing a rush to offensive cyberweapons. Future work by the International Committee of the Red Cross or by nongovernmental organizations such as the EastWest Institute might pave the way for such a recognition by China as well.

The experts group report reiterates the statement from the report of the 2010 experts group of the need for common understandings on how such norms apply to state behavior and the use of ICTs by states, as well as the possibility of developing more-specific rules of behavior.

**Building Transparency and Trust**

On the controversial issue of how to deal with the increasing likelihood that countries will pursue development of cyberweapons, the group managed to take a realistic approach. In their draft code of conduct regarding the use of ICTs by states, submitted to the UN secretary-general in 2011, China and Russia suggested explicit prohibitions of what they term “information weapons” and the proliferation of their technologies.\[12\]

Yet, in the course of the experts group deliberations, the Chinese and Russian representatives recognized the inherently dual nature of these technologies and joined the more pragmatic approach of starting out with traditional confidence-building measures and other cooperative measures before attempting to agree on prohibitions that are basically unverifiable. At the same time, the experts understood that confidence-building measures can be a starting point should an arms control approach become feasible in the future.

In several paragraphs, the group’s 2013 report refers to language used in other treaties with arms control implications. In particular, the report calls on states to promote a “peaceful” ICT environment, which could be understood as an allusion to the so-called “peaceful purpose” clause of the Outer Space Treaty. In its approach to cyberspace issues, the experts group applies a similar concept by refraining from imposing specific prohibitions but positing the general objective of peaceful state use of cyberspace. This strengthens the ability of future agreements to cover future developments in the field.

Recognizing that confidence-building measures and the exchange of information among states are essential to increasing predictability and reducing the risks of misperception and escalation through cyberthreats, the experts group agreed on a range of voluntary measures to promote transparency and confidence among states in this area. The measures are aimed at increasing transparency and creating or strengthening communication links in order to reduce the possibility that a misunderstood cyberincident could create international instability or a crisis leading to conflict. Taken together, they represent an important foundation for bilateral, regional, and global measures to build confidence and global stability in cyberspace and to prevent unnecessary escalation of cybersecurity incidents.

In particular, the report recommends the following confidence-building measures:

- Exchanging views and information on national policies, best practices, decision-making processes, and national organizations and structures with regard to cybersecurity. As an example, the United States in 2012 and Germany in 2013 exchanged so-called white papers on cyberdefense with Russia.
• Creating bilateral or multilateral consultative frameworks for confidence-building measures, for example, within the Arab League, the African Union, the Association of Southeast Asian Nations (ASEAN) Regional Forum, the Organization for Security and Co-operation in Europe (OSCE), and the Organization of American States. These frameworks could include workshops and exercises on how to prevent and manage disruptive cybersecurity incidents.

• Enhancing the sharing of information and crisis communication among states on cybersecurity incidents at three levels: between national CERTs bilaterally and within already existing multilateral CERT communities to exchange technical information about malware or other malicious indicators; through previously existing or newly created channels for crisis management and early warning to receive, collect, analyze, and share such information to help mitigate vulnerabilities and risks; and through channels for dialogue at political and policy levels.

• Increasing cooperation to address incidents that affect critical infrastructure systems, particularly those that rely on ICT-enabled industrial control systems.

• Enhancing mechanisms for law enforcement cooperation to reduce incidents that could be misunderstood as hostile state actions and that affect international security.

Although governments must take the lead in developing and implementing these measures, the group reiterates and highlights the important role the private sector and civil society should play in these efforts. In future work, governments and the private sector must undertake joint efforts to elaborate the objectives, conditions, requirements, frameworks and models of such public-private partnerships for international cybersecurity on a global scale. Some global ICT companies already are engaged in this discussion. Yet, the specific roles of states and private companies and the limitations on cooperation among them in the sensitive field of cybersecurity need to be more clearly developed by governments and private sector stakeholders.

In its report, the experts group highlights the need for international capacity building to help states in their efforts to overcome the digital divide and to improve the security of vital ICT infrastructure. The report calls on states, working with the private sector and UN specialized agencies, to provide technical or other assistance in building capacities in ICT security. In particular, such assistance could help to strengthen national legal frameworks and law enforcement capabilities and strategies, combat the use of ICTs for criminal or terrorist purposes, and strengthen incident response capabilities, including through CERT-to-CERT cooperation.

**Outlook**

The experts group report gives the UN and its member states a unique opportunity to advance toward a more predictable, secure, and peaceful international cyberspace. The report recommends that the UN pursue regular, ongoing institutional dialogue “with broad participation” to enhance common understandings and intensify practical cooperation on global cybersecurity. By emphasizing the “broad” character of the future dialogue, the report appears to be foreshadowing a larger group of experts.

This fall, the UN General Assembly probably will take up a resolution in the First Committee to set up another experts group in 2014, possibly with 25 members. By tradition, that group would include the five permanent members of the Security Council and other interested states selected by the secretary-general on the basis of geographical balance and other criteria. It probably would be mandated to more specifically address issues of international humanitarian law in relation to cyberactivities that could reach the level of armed conflict, particularly how to protect civilian populations from unintended effects of cyberattacks against military targets. Therefore, it should have more regular recourse to advice by legal experts.

In addition, member states and regional organizations now have a set of recommendations for cooperation, conflict prevention, and confidence building that could be agreed bilaterally or multilaterally, following the successful U.S.-Russian model of this past June. The chances that the OSCE will agree to a first set of confidence-building measures by the end of December are better than they were a year ago when the Russian delegation was still raising definitional and ideological objections in the organization’s informal working group on cybersecurity. In July 2012, the ASEAN Regional Forum adopted a forward-looking ministerial statement on cybersecurity. As in the
The UN Takes a Big Step Forward on Cybersecurity
Published on Arms Control Association (https://www.armscontrol.org)

OSCE, this commitment could be fleshed out in the coming months by agreeing on measures for building confidence and improving states’ capacities for building resilient ICT infrastructures to ensure that cyberspace activity is peaceful.

The UN has taken a big step toward shaping an urgently needed international framework for legitimate and prosperous activities in cyberspace while offering the entire UN membership the tools to prevent a hasty militarization of the domain. Yet, this is only a beginning. Member states must make sure to undergird this framework with state practices fully in line with the general purpose criterion to make cyberspace “peaceful, secure, open and cooperative,” the goal articulated in the experts group report.

Detlev Wolter was director for conventional arms control and confidence- and security-building measures in the German Foreign Office from August 2010 to July 2013. He served as one of the 15 experts on the UN group of governmental experts on information and telecommunications in the context of international security. The views expressed in this article are those of the author.

ENDNOTES


The UN Takes a Big Step Forward on Cybersecurity
Published on Arms Control Association (https://www.armscontrol.org)

8. UN experts group cybersecurity report, para. 11.

9. Legal attribution would require either that a state organ itself has directed the cyberattack or that it has control over the nonstate group that directed it. Technical attribution would require identification of the computers from which the malware originated and of the perpetrators behind the malware.

10. The law of armed conflict, also known as international humanitarian law, applies when there is a use of force. Under Article 51 of the UN Charter, the threshold for self-defense is “armed attack.”


12. Russia and China information security letter.

13. UN experts group cybersecurity report, para. 29.


Source URL: https://www.armscontrol.org/act/2013-09/un-takes-big-step-forward-cybersecurity