04

CYBERSECURITY AND INTERNATIONAL PEACE AND SECURITY

VLADIMIR RADUNOVIĆ, DIPLO FOUNDATION

INTRODUCTION

States have been discussing the effects of information and telecommunications technology on international peace and security since the 1990s. Since then, several significant cyber incidents made front-page headlines and a growing number of governments have been developing new policies and institutions on the political and military use of cyberspace. As a result, an active debate is now taking place about what norms should govern behaviour in cyberspace, how to build confidence and increase stability, and how to build up the capacity of states to address cybersecurity threats within their own borders. This debate includes a number of important human rights considerations. This webinar is designed to help build understanding of the issues, the actors in play, and where and when this topic is being discussed.

THE WHAT – WHAT IS THE TOPIC ABOUT?

An increasing number of states have been integrating cybersecurity into their national security and defense strategies and some have gone so far as to implement separate defense and security strategies for cyberspace. This rise of cybersecurity from low to high politics has brought about new investment in national capacity to respond to threats and vulnerabilities and in developing cyber-offensive and defensive military capabilities. Because of heightened interest and investment at the national level, questions emerged around the applicability of traditional security concepts, laws, and governance structures to cyberspace. The discourse revolves around laws, norms, and principles that govern state action in cyberspace, confidence building measures (CBMs) for cyberspace, and capacity building measures for cyberspace.

THE WHY – WHY IS THIS TOPIC IMPORTANT FROM A HUMAN RIGHTS PERSPECTIVE?

The cybersecurity debate from the perspective of international peace and security is important for human rights proponents and humanitarians because it focuses on the norms, laws, and principles governing state actions in cyberspace. This includes, for example, discussions on how existing principles such as the principle of distinction (the concept that militaries must differentiate between civilian and military targets), or the principle of proportionality (the concept that the destruction caused by an attack must be proportionate to the military gain achieved from that attack) apply to cyberspace. Without mature versions of these concepts and others, state action in cyberspace is potentially anarchical, and the ability of states to carry out attacks on civilians is legally and normatively untethered. Furthermore, many proposals for new laws to govern state action in cyberspace propose to codify the state's role in controlling information online. These measures pose specific threats to free expression around the world. That is why the discussion about how to define information security and cybersecurity has important human rights implications. Moreover, there are opportunities for civil society engagement on the topic of cybersecurity and international peace and security which governments have explicitly acknowledged, for example, in the context of the CBMs discussion at the Organization for Security and Co-operation in Europe (OSCE) or the UN General Assembly's First Committee.

THE HOW – HOW IS THIS TOPIC BEING ADDRESSED?

The laws, norms, and principles that govern state action in traditional conflict are grounded in a strong recognition of the value of human lives and the importance of human rights. Similar to the discussion over whether human rights apply offline as well as online and the resolution adopted by the UN Human Rights Council, there has been a debate over whether the norms codified in international humanitarian law apply offline as well as online. Some states contested that international humanitarian law applies online as well as offline until a group of governmental experts (UNGGE) from 15 countries established by the UN General Assembly's First Committee agreed that international law is applicable in a consensus report published in 2013.

Arguably the more challenging aspect of the norms discussion is how to interpret existing international law for cyberspace and what norms might have to be developed for activities that are not covered by existing law. The Tallinn Manual on the International Law Applicable to Cyber Warfare published in 2013 focus on this translation exercise. It was developed by an independent group of 15 legal experts under the auspices of NATO's Cooperative Cyber Defence Centre of Excellence. A new group is currently in the process of looking into the types of activities where there is a greater uncertainty of what type of law and norms apply.

Complementing this norms discussion is the diplomatic effort to develop CBMs for cyberspace. The OSCE adopted the first multilateral set of CBMs in December 2013. The concept of CBMs dates back to the Cold War and describes the efforts by superpowers to avoid accidental escalation or nuclear war due to misunderstandings. CBMs are designed to prevent unnecessary conflict in terms of both scale and incidence. States and other actors are now trying to develop CBMs to reduce the likelihood of conflict in cyberspace.

THE WHO, WHERE AND WHEN – WHO ARE THE MAIN PLAYERS, WHERE AND WHEN IS THE TOPIC BEING ADDRESSED?

Cybersecurity from an international peace and security perspective has been discussed in various international fora including the UN General Assembly, the G8, the London Conference process and regional organisations such as the OSCE, NATO, the Shanghai Cooperation Organization, and the Association of Southeast

Asian Nations Regional Forum.

One of the key fora is the UN General Assembly's First Committee that has been discussing developments in the field of information and telecommunications in the context of international security since 1998. This process also led to the creation of groups of governmental experts (UNGGE). A fourth group is currently in place consisting of representatives from 20 countries and expected to publish its report in the second half of 2015. It was preceded by three UNGGEs and the report published by the third UNGGE in 2013 remains the most significant because of its affirmation of existing international law, sovereignty, human rights, and governance.

In 2011, China, Russia, Tajikistan, and Uzbekistan submitted a draft version of an International Code of Conduct for Information Security, a proposal developed through the Shanghai Cooperation Organization (SCO) for new norms and laws governing state conduct in cyberspace, to the UN General Assembly. Shortly following the initial submission of the Code of Conduct, Russia also presented a draft Convention on International Information Security, which sparked debate regarding the need for a "treaty for cyberspace." In January 2015, the SCO proposed an updated draft of the Code of Conduct calling on states to prevent the use of information technologies to spread information that "incites terrorism, separatism or extremism or that inflames hatred on ethnic, racial or religious grounds." Because states define and interpret words like terrorism, separatism, and extremism in different ways, many governments and human rights experts are concerned that language like the proposed Code of Conduct would be used by states to legitimise limiting free speech and expression.

NATO has also actively discussed cybersecurity and its implications for international security. In September 2014, NATO heads of state agreed that Article 5 of the defense treaty, the collective defense clause, applies to cyber attacks as it does to conventional attacks, though they refrained from defining what kinds of attacks would invoke the clause. In addition, the Tallinn Manual on the International Law Applicable to Cyber Warfare, developed by an independent group of 15 legal experts under the auspices of NATO's Cooperative Cyber Defence Centre of Excellence, spun out of the discussions at NATO following the 2007 Distributed Denial of Service attacks targeting Estonia.

Another important forum where cybersecurity has been discussed through the lens of international peace and security is the London Process which started with the 2011 London Cybersecurity Conference. The Global Conference on Cyberspace in The Hague is the fourth conference in this series following the second conference in Budapest, Hungary, in 2012 and the third conference in Seoul, Republic of Korea, in 2013. The goal of the Global Conference on Cyberspace is "to promote practical cooperation in cyberspace, to enhance cyber capacity building, and to discuss norms for responsible behaviour in cyberspace."

SUGGESTED LITERATURE

- Kavanagh, Camino, Tim Maurer and Eneken Tikk-Ringas. Baseline Review of ICT-Related Processes and Events: Implications for International and Regional Security. 2013. Available at: http://ict4peace.org/baseline-review-of-ict-related-processes-and-events-implications-for-international-and-regional-security/