# I. Cyber Security and Protecting Against Cyber Warfare

***Introduction***

Ensuring international peace and security in cyberspace is currently one of the most prevalent topics of discussion due to the plethora of cyberattacks that threaten countries' stability and overall sustainable development.[77] The United Nations (UN) system acknowledged that the efforts of the General Assembly First Committee to ensure international peace and security have to focus particularly on securing critical cyber infrastructure and information and communications technologies (ICTs) that dominate everyday life.[78] The threat not only stems from possible escalation of cyber warfare among states but also criminal and terrorist activities in cyberspace.[79] Terrorist organizations use the cyber sphere to spread their messages, mobilize human and financial resources, and to directly attack critical infrastructure, such as hospitals, water systems, energy, or financial services, to harm states and their people.[80] However, in an effort to ensure cyber security, some Member States have taken up measures that violate fundamental human rights recognized in the 1948 *Universal Declaration of Human Rights* (UDHR).[81]

The term cyber security commonly comprises "the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance, and technologies that can be used to protect the cyber environment and organization and user's assets."[82] Protecting the cyber sphere against the threat of cyberattacks, cyber warfare, cybercrime, and cyber terrorism, has become a priority for the international community.[83] However, these concepts are often used interchangeably and lack internationally agreed-upon definitions.[84] The UN Institute for Disarmament Research (UNIDIR) defines cyberattacks "as the unauthorized penetration of computers or digital networks."[85] Cyberattacks have grown more sophisticated, reaching alarming levels of disruption on a global scale while, at the same time, requiring only simple and easily attainable technology.[86] Threats have increased continuously to a new five-year high as the proliferation of mobile devices, artificial intelligence, robotics, and the Internet of Things brings new vulnerabilities.[87]

Cyber criminals span from "state-sponsored cyber espionage groups to mass-mailing ransomware gangs."[88] Cybercrime describes "any illegal behavior directed by means of electronic operations that target the security of computer systems, the data processed by them (...) illegal possession and offering or distributing information by means of a computer system or network."[89] Cyber warfare requires the involvement of a state "to attack and attempt to damage another state's computers or information networks through, for example, computer viruses or denial-of-service attacks."[90] However, cybercrime and cyber warfare are difficult to differentiate as hacking groups engaging in criminal activities against individuals are also often supported by governments to engage in cyber espionage against Member States.[91] The act of cyber terrorism is mostly distinguished by the motives of the perpetrators.[92] It is often understood as "the use of computer network tools to shut down critical national infrastructures (such as energy, transportation, government operations) or to coerce or intimidate a government or civilian population."[93] To

[77] UN ITU, *Global Cybersecurity Agenda (GCA)*, 2007, p. 2; Smart, *United Nations Office for Disarmament Affairs*, 2016.
[78] Smart, *United Nations Office for Disarmament Affairs*, 2016.
[79] Ibid.
[80] Ibid.; UN CTITF, *Countering the Use of the Internet for Terrorist Purposes – Legal and Technical Aspects*, 2011.
[81] Smart, *United Nations Office for Disarmament Affairs*, 2016; UN General Assembly, *Universal Declaration of Human Rights (A/RES/217A (III))*, 1948; Radunovic, *Cybersecurity and International Peace and Security*, 2015.
[82] UN ITU, *Understanding cybercrime: Phenomena, Challenges and Legal Response*, 2014, p. 7.
[83] Lewis & Neuneck, *The Cyber Index: International Security Trends and Realities*, 2013.
[84] Lewis, *Confidence-building and international agreement in cybersecurity*, 2011, p. 57.
[85] Lewis & Neuneck, *The Cyber Index: International Security Trends and Realities*, 2013, p. x.
[86] Symantec, *Internet Security Threat Report 2017*, 2017, pp. 7-8.
[87] Ibid., pp. 63-72.
[88] UN ITU, *Global Cybersecurity Index (GCI) 2017*, 2017, p. 1.
[89] UN ITU, *Understanding cybercrime: Phenomena, Challenges and Legal Response*, 2014, p. 11.
[90] RAND, *Cyber Warfare*, 2017.
[91] Beaver, The United Nations and Cyberwarfare, *Global Risk Advisors*, 2017.
[92] Brenner, *At Light Speed: Attribution and Response to Cybercrime/Terrorism/Warfare*, 2007, pp. 386-400.
[93] Lewis, *Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats*, 2002, p. 1.

ensure international peace and security, it is important that the General Assembly First Committee continues its efforts to secure cyberspace and critical cyber infrastructure from all forms of cyberattacks.[94]

***International and Regional Framework***

The international community has been debating cyber security for the last two decades.[95] The General Assembly in particular developed an elaborate international framework, adopting annual resolutions around the issue of ICTs and international security since 1999.[96] The first, resolution 53/70, recognized the potential of ICTs for peoples' development but also noted threats to international order and peace that may arise through the misuse of ICTs.[97] The General Assembly expanded on its original resolution by establishing a group of governmental experts in resolution 58/32 and addressing respect for human rights and fundamental freedoms regarding ICTs in resolution 70/237.[98] In 2000, the General Assembly laid the foundations on "combating the criminal misuse of information technologies" highlighting effective legal regimes, prosecution, and information sharing and cooperation among Member States to ensure that ICTs contribute to international development rather than undermining it.[99] Another collection of noteworthy General Assembly resolutions, 57/239, 58/199, and 64/211, were adopted between 2003 and 2010 on the "creation of a global culture of cybersecurity" addressing Member States' capacity to safeguard their critical information infrastructures from cyberattacks.[100] These documents indicate an important shift from mere law enforcement practices and prosecution of cybercrimes to the prevention of attacks in the cyber sphere and requested a more firm commitment from Member States to secure cyber space and address growing cyber threats.[101]

In 2007, the International Telecommunications Union (ITU) introduced the Global Cybersecurity Agenda (GCA), which serves as a practical framework for all 193 Member States and more than 700 Sector Members to collaborate on cyber security.[102] The GCA consists of five pillars.[103] First, "legal measures" focuses on the persecution of unlawful cyber activities with an internationally consistent legislative approach.[104] Second, "technical and procedural measures" looks at the security standards of ICT applications and systems and best practices of risk management.[105] Third, "organizational structures" discusses national policies, and institutional setups allowing for an effective prevention, response to, and crisis management of cyberattacks.[106] Fourth, "capacity building" promotes awareness and technology sharing among all stakeholders.[107] And the last pillar, "international cooperation," promotes dialogue and coordinated action of the international community in dealing with cyber threats.[108]

In the context of the *2030 Agenda for Sustainable Development* (2016), the usage of ICTs, and therefore their safeguarding, is critical considering their catalyst role for sustainable development.[109] Four of the 17 Sustainable

---

[94] Tikk-Ringas, *Developments in the Field of Information and Telecommunication in the Context of International Security: Work of the UN First Committee 1998-2012*, 2012, p. 10.
[95] UNODA, *Developments in the field of information and telecommunications in the context of international security*, 2017; UN ITU, *UN Resolutions Related to Cybersecurity*, 2017; Maurer, *Cyber Norm Emergence at the United Nations*, 2011, p. 15.
[96] Ibid.
[97] UN General Assembly, *Developments in the field of information and telecommunications in the context of international security (A/RES/53/70)*, 1999.
[98] UN General Assembly, *Developments in the field of information and telecommunications in the context of international security (A/RES/58/32)*, 2003; UN General Assembly, *Developments in the field of information and telecommunications in the context of international security (A/RES/70/237)*, 2015.
[99] UN General Assembly, *Combating the criminal misuse of information technologies (A/RES/55/63)*, 2001.
[100] UN General Assembly, *Creation of a global culture of cybersecurity (A/RES/57/239)*, 2003; UN General Assembly, *Creation of a global culture of cybersecurity and the protection of critical information infrastructure (A/RES/58/199)*, 2004; UN General Assembly, *Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructure (A/RES/64/211)*, 2010.
[101] Ibid.
[102] UN ITU, *Global Cybersecurity Agenda (GCA)*, 2007.
[103] Ibid., p. 2.
[104] Ibid., pp. 6-9.
[105] Ibid., pp. 9-12.
[106] Ibid., pp. 12-13.
[107] Ibid., pp. 13-15.
[108] Ibid., pp. 15-19.
[109] UN DESA, *ICTs as a catalyst for sustainable development*, 2016.

Development Goals (SDGs) include explicit targets regarding the use of ICTs (SDGs 4, 5, 9, 17).[110] In addition, SDG 16 targets the prevention of terrorism and crime which are also prevalent in cyberspace.[111] As policymakers and the ICT sector strive to connect the billions of people that are still lacking access to ICTs and the achievement of all SDGs depends on technological innovation and transformative digital services, cyber security always needs to be taken into consideration.[112]

The first legally binding agreement governing cyberspace was made on a regional level by the Council of Europe (CoE) which adopted the *Budapest Convention on Cybercrime* in 2001, entering into force in 2004.[113] To this date, almost all CoE Member States have both signed and ratified the convention with the exception of Ireland, Russia, Sweden, and San Marino.[114] There are also a number of non-members that have become States parties to the convention such as the United States of America.[115] The Budapest Convention is the first international treaty that outlines policies and legislation protecting against cybercrime focusing on the effective prosecution of offenses and encouraging closer cooperation among Member States to address common threats to cyber security.[116] In 2014, the *African Union (AU) Convention on Cyber Security and Personal Data Protection* established a standard legal framework for aspects such as online business and digital privacy while addressing emerging issues of cyber security and cybercrime.[117] Regulating cyber space and mitigating risks are crucial to guarantee safe usage of ICTs, which are an important driver for African development.[118] However, as of June 2017, only Senegal has ratified the convention and many have voiced concerns that domestic cyber legislation derived from the convention may disregard the protection of human rights enshrined in the UDHR, particularly of the freedom of expression, under the disguise of cyber security.[119]

***Role of the International System***

In 2004, the General Assembly First Committee installed the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (GGE).[120] The GGE is a UN-mandated working group comprised of 15 experts appointed by the Secretary-General examining potential and existing cyber threats.[121] Russia and its allies advocated early on for the First Committee to "address a wider spectrum of threats to include military, terrorist, and criminal uses of ICT," while the United States and other Western countries preferred a more limited role of the First Committee in information security.[122] These opposing views left the GGE without any advances until 2009.[123] Since then the GGE has met four times and published three reports in 2010, 2013, and 2015.[124] A crucial point made in the 2010 report (A/65/201) concerns the "increased reporting that States are developing ICTs as instruments of warfare and intelligence, and for political purposes."[125] The GGE has produced guidelines and recommendations regarding norms and principles of state behavior and accountability for their actions in the digital sphere.[126] Other important aspects are the applicability of international law to ICTs and cyberspace; state sovereignty; international cooperation and information sharing to build capacity

---

[110] Ibid.
[111] UN DESA, *Sustainable Development Goal 16*, 2017.
[112] Earth Institute & Ericsson, *ICT & SDGs*, 2016.
[113] Council of Europe, *Convention on Cybercrime*, 2001.
[114] Council of Europe, *Chart of signatures and ratifications of Treaty 185*, 2017.
[115] Ibid.
[116] Council of Europe, *Convention on Cybercrime*, 2001.
[117] African Union, *African Union Convention on Cyber Security and Personal Data Protection*, 2014.
[118] Fidler & Madzingira, The African Union Cybersecurity Convention: A Missed Human Rights Opportunity, *Council on Foreign Relations*, 2015.
[119] Ibid.
[120] Tikk-Ringas, *Developments in the Field of Information and Telecommunication in the Context of International Security: Work of the UN First Committee 1998-2012*, 2012, pp. 5-6.
[121] Ibid.
[122] Ibid, p. 5.
[123] Ibid, pp. 7-9.
[124] Ibid.; UNODA, *Developments in the field of information and telecommunications in the context of international security*, 2017.
[125] UN General Assembly, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (A/65/201)*, 2010, p. 7.
[126] GIP Digital Watch, *UN GEE*, 2017.

and reduce vulnerabilities; and confidence-building measures to uphold international peace.[127] The recent 2016-17 GGE consultations addressed further development of international law and norms that should guide Member States' conduct in cyberspace, though the negotiations ended without the adoption of a final report.[128] While there was agreement on a number of points the members were unable to come to a consensus on what options Member States might have to respond to cyberattacks, and if and how to take the process further under the UN.[129] The future of the GGE and finding compromise on an approach to cyber security, including prevention and response to cyber warfare, cybercrime, and cyber terrorism, are still to be discussed by the First Committee.[130] Discussions on the issue of information warfare and cyber weapons and the need for disarmament and non-proliferation hereof have fallen into the background debates regarding criminal and terrorist use of ICTs.[131]

The ITU, whose mandate is to help build confidence and security in the use of ICTs, plays a crucial role in identifying and mitigating modern cyber threats.[132] Its mandate is to help build confidence and security in the use of ICTs.[133] The ITU supports national cyber security capacity through establishing National Computer Incident Response Teams.[134] To further cooperation among governments, the ITU promotes the creation of Regional Cybersecurity Centres and regional cyber security summits strengthening the knowledgebase of Member States, helping them develop cyber security strategies and initiatives, and localizing ITU's cyber security services, such as conducting drills simulating effective responses to cyber threats.[135] In 2017, the ITU published the new Global Cybersecurity Index (GCI) that assesses Member States' commitment to the five strategic pillars of cyber security.[136] In addition, the ITU hosts the annual World Summit on Information Society (WSIS) Forum that focuses on the achievement of sustainable development through ICTs.[137] The June 2017 WSIS Forum led a debate on the possibility for such a treaty complementing existing international law.[138] Proponents of a cyber convention argue that the room for interpretation and ambiguity is too great, although many experts and Member States argue that a digital convention is neither necessary nor realistic and existing guidelines are sufficient to govern responsible state behavior in cyberspace.[139]

Though traditionally tasked with nuclear disarmament as well as other physical weapons, the United Nations Office for Disarmament Affairs (UNODA) has closely monitored the work of the General Assembly and the Secretary-General on information security.[140] It particularly offers expertise in the area of military confidence-building.[141] This expertise could be applied to cyber security, using confidence-building measures (CBMs) to address trust among states' regarding each other's cyber warfare capabilities.[142] Non-military CBMs in this context include actions in various aspects of cyber security to create trust between parties due to increased transparency.[143] UNIDIR conducts relevant research and analysis in the field of cyber security and offers policy recommendations at the national, regional, and international level.[144] Important projects include legal perspectives on cyber war, the questions of

---

[127] Ibid., UNODA, *Developments in the field of information and telecommunications in the context of international security*, 2015.
[128] GIP Digital Watch, *UN GEE*, 2017.
[129] Ibid.
[130] GIP Digital Watch, *Digital Policy Trends in June*, 2017, p. 6.
[131] Tikk-Ringas, *Developments in the Field of Information and Telecommunication in the Context of International Security: Work of the UN First Committee 1998-2012*, 2012, p. 7.
[132] UN ITU, *ITU Cybersecurity Activities*, 2017.
[133] Ibid.
[134] Ibid.
[135] UN ITU, *Regional Cybersecurity Centres*, 2017; UN ITU, *ITU Cybersecurity Activities*, 2017.
[136] UN ITU, *Global Cybersecurity Index (GCI) 2017*, 2017.
[137] UN ITU, *ITU Cybersecurity Activities*, 2017.
[138] WSIS, *WSIS Forum 2017: Information and Knowledge Societies for SDGs – Outcome Document*, 2017.
[139] NATO CCDCOE, *Geneva Conventions Apply to Cyberspace: No Need for a 'Digital Geneva Convention'*, 2017; Tikk-Ringas, *Developments in the Field of Information and Telecommunication in the Context of International Security: Work of the UN First Committee 1998-2012*, 2012, p. 6.
[140] UNODA, *Developments in the field of information and telecommunications in the context of international security*, 2017.
[141] Ibid.
[142] UNODA, *Military Confidence-building*, 2017.
[143] Lewis, *Confidence-building and international agreement in cybersecurity*, 2011, pp. 56, 59; Lewis & Neuneck, *The Cyber Index: International Security Trends and Realities*, 2013, pp. 129-130.
[144] UNIDIR, *Cyber*, 2017.

cyber norms and the applicability of international law to cyberspace, as well as confidence-building and active prevention of the proliferation of malicious ICT tools and techniques.[145]

On the international level, there are other multilateral organizations and initiatives that address cyber security and cyber defense. For example, the North Atlantic Treaty Organization (NATO) established a Cooperative Cyber Defence Centre of Excellence (CCDCOE) that conducts research and training regarding cyber defense informing NATO's policies and action plan on resilience and protection of critical networks against cyberattacks.[146] In 2013, the CCDCOE prepared the Tallinn Manual on the International Law Applicable to Cyber Warfare, which focused on cyber war and the prohibition of the use of force as well as Member States right to self-defense in this regard.[147] The manual has been updated as Tallinn Manual 2.0 (2017), expanding specifically on cyber threats and recurring attacks in cyberspace against governments, the private sector, and citizens.[148] The Commonwealth Cybercrime Initiative, a consortium of 35 organizations, uses its convening power to foster cooperation and its technical expertise to assist members in national needs assessments and priority setting regarding cyber security.[149] Lastly, the Global Forum on Cyber Expertise, comprised of 60 organizations and states, aims to formulate a shared global agenda on cyber capacity building.[150] To this end, it partnered with the Global Cyber Security Capacity Centre creating a new global platform promoting cyber capacity building.[151]

***Strengthening Cyber Security and Prevention Strategies***

Achieving global cyber security and ensuring peace in cyberspace is a significant challenge.[152] The recent "WannaCry" ransomware strike, in which hackers gained access to and encrypted great amounts of personal data and files, hospital records, and train systems, and demanded a ransom from citizens and institutions if they were to receive access again, affected more than 150 countries.[153] Global disruptions like these can pose a real threat to international peace and security, especially if they target the digital systems of militaries or nuclear energy facilities.[154] One possibility discussed by UNIDIR to protect countries from such attacks is the prevention of the proliferation of malicious ICT tools and techniques.[155] In addition, effective measures are needed to improve the resilience of networks and guard them from such criminal activities in the first place.[156] The ITU GCI 2017 revealed that huge gaps in security still persist.[157] Though the UN has consistently called upon its Member States to formulate and implement a national cyber security or cyber defense strategy, 50% of the examined countries have not yet developed such a strategy.[158] The ITU recommends that national strategies outline policies to identify cyber risks and threats, mitigation strategies, and develop defense mechanisms in the event of a cyberattack.[159] Further, they can assist governments in setting priorities and include objectives toward legal frameworks, early warning and response mechanisms, capacity building and training, research and development, and international collaboration.[160]

Capacity building goes hand-in-hand with international collaboration, as developing countries require assistance to safeguard their networks and cyber infrastructure.[161] Cooperation among Member States is a crucial element of the

---

[145] UNIDIR, *Report of the International Security Cyber Issues Workshop Series*, 2016.
[146] NATO, *Cyber defence*, 2017.
[147] NATO CCDCOE, *Geneva Conventions Apply to Cyberspace: No Need for a 'Digital Geneva Convention'*, 2017; NATO CCDCOE, *Tallinn Manual on the International Law Applicable to Cyber Warfare*, 2013.
[148] NATO CCDCOE, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 2017.
[149] Commonwealth Secretariat, *Commonwealth Cybercrime Initiative*, 2017.
[150] Global Forum on Cyber Expertise, *Working towards a global cyber capacity building agenda in 2017*, 2017.
[151] Global Cyber Security Capacity Centre, *Cybersecurity Capacity Portal*, 2017.
[152] Beaver, The United Nations and Cyberwarfare, *Global Risk Advisors*, 2017.
[153] UN DPI, *In wake of 'WannaCry' attacks, UN cybersecurity expert discusses Internet safety*, 2017.
[154] UNIDIR, *Report of the International Security Cyber Issues Workshop Series*, 2016.
[155] Ibid.
[156] UN DPI, *Half of all countries aware but lacking national plan on cybersecurity, UN agency reports*, 2017.
[157] UN ITU, *Global Cybersecurity Index (GCI) 2017*, 2017.
[158] UN DPI, *Half of all countries aware but lacking national plan on cybersecurity, UN agency reports*, 2017.
[159] Ibid.
[160] CERT India, *Cyber Security & Role of Cert-In*, 2009, p. 14.
[161] UN General Assembly, *Developments in the field of information and telecommunications in the context of international security (A/RES/71/28)*, 2016; UN General Assembly, *Developments in the field of information and telecommunications in the context of international security – Report of the Secretary-General (A/71/172)*, 2016.

GGE recommendations.[162] Political will to share cyber capabilities is lacking, especially between countries considering cyberattacks on each other.[163] Therefore, another strategy recommended by the GGE is to pursue the development of CBMs among states.[164] Conventional CBMs deescalate tensions between countries and aim to build mutual trust by increasing transparency about national military capacities.[165] A similar approach might be possible regarding cyber capacities to avoid conflict.[166] To date, General Assembly resolution 71/39 on "CBMs in the regional and subregional context" makes no mention of cyber-related actions.[167] The Organisation for Security and Co-operation in Europe has advanced efforts on specifying a list of CBMs For Cyberspace that aim primarily at voluntary information sharing on issues pertaining ICT security.[168]

***Responding to Cyberattacks***

While the development of legal frameworks and means of domestic prosecution of cybercrimes has seen substantial progress, military responses still need extensive deliberation in the international arena.[169] There has been no consensus in the GGE on acceptable options Member States may use to respond to cyberattacks perpetrated by or with the involvement of states.[170] The involvement of a state or its favorable view on the attack can complicate investigation and prosecution of cyberattacks committed by criminals and terrorists if they receive protection from the respective country.[171] The First Committee has yet to define categories and thresholds of what constitutes an act of war in cyberspace and which countermeasures are appropriate.[172] Developing a catalogue of measures to respond to cybercrimes, cyber terrorism, and cyber warfare is an enormous political and diplomatic challenge.[173]

Attribution in cyberspace is difficult and most countries lack the technological know-how to do so.[174] However, applying international law requires sound evidence of the attacking party.[175] To avoid escalation into cyber war, experts at UNIDIR propose a norm that allows the affected state to only take actions, which have yet to be determined, that do not involve the use of force in responding or retaliating to a cyberattack.[176] If the aggressor is a Member State, some experts suggest involving the Security Council and imposing sanctions.[177] This calls for the definition of a threshold for the damage an attack has caused to justify certain Security Council activities, though said damage may not always be of physical nature, but rather financial or political.[178] The attack may still be considered an act of war by the affected state, opening a discussion around the right to self-defense.[179] Though a single attack may not reach a critical threshold, concerted efforts to weaken the economy or the political stability of a country could potentially be considered a cyberwarfare campaign.[180] Notwithstanding the need to protect against and respond to cyber warfare, the First Committee has not sufficiently discussed the issue of self-defense, appropriate responses to cyberattacks that target national critical cyber infrastructure, and how to avoid escalation.[181] The EU has created a cyber diplomacy toolbox that offers guidance on how to address cyberattacks that do not meet

---

[162] GIP Digital Watch, *UN GEE*, 2017.
[163] Beaver, The United Nations and Cyberwarfare, *Global Risk Advisors*, 2017.
[164] GIP Digital Watch, *UN GEE*, 2017.
[165] UNODA, *Military Confidence-building*, 2017.
[166] Lewis, *Confidence-building and international agreement in cybersecurity*, 2011.
[167] UN General Assembly, *Confidence-building measures in the regional and subregional context (A/RES/71/39)*, 2016.
[168] NATO CCDCOE, *OSCE Expands Its List of Confidence-Building Measures For Cyberspace: Common Ground on Critical Infrastructure Protection*, 2016.
[169] Brenner, *At Light Speed: Attribution and Response to Cybercrime/Terrorism/Warfare*, 2007, pp. 440-474.
[170] GIP, Digital Watch, *Digital Policy Trends in June*, 2017; Brenner, *At Light Speed: Attribution and Response to Cybercrime/Terrorism/Warfare*, 2007, pp. 421-424.
[171] Brenner, *At Light Speed: Attribution and Response to Cybercrime/Terrorism/Warfare*, 2007, pp. 421-424.
[172] UNIDIR, *Report of the International Security Cyber Issues Workshop Series*, 2016.
[173] Ibid.
[174] Ibid., pp. 9-10.
[175] Ibid, pp. 15-16.
[176] Ibid, p. 17.
[177] Ibid.
[178] Ibid.
[179] Beaver, The United Nations and Cyberwarfare, *Global Risk Advisors*, 2017.
[180] Ibid.
[181] Tikk-Ringas, *Developments in the Field of Information and Telecommunication in the Context of International Security: Work of the UN First Committee 1998-2012*, 2012, p. 10.

the threshold of an armed attack.[182] However, the EU struggles to streamline its cyber security policies into one coherent approach responding to an actual attack on its critical cyber infrastructure.[183] It also lacks coordination with cyber defense strategies of NATO and remains ad hoc in nature.[184]

***Conclusion***

Cyber security impacts all spheres of life, and sustainable development is dependent on the innovative use of ICTs.[185] However, with the emergence of new technologies there is always a chance that these advancements are used against a country and their people threatening international peace and security.[186] Differentiating between the concepts of cyber warfare, cybercrime, and cyber terrorism has proven difficult.[187] No internationally agreed definitions exist for these terms.[188] Part of the problem is often the inability to conclusively attribute a cyberattack to one specific actor or to potentially link criminal activities by hacker groups to governments, effectively blurring the lines between cybercrime and cyber warfare.[189] The General Assembly First Committee has made slow progress on cyber security over the last 20 years. Even though the need for capacity building and international cooperation has long been recognized by the committee, the lack of trust among Member States and universally agreed cyber norms impede further advancement.[190] This is aggravated by the fact that half of the world has not yet formulated national cyber security or cyber defense strategies and do not realize the potential cyber threats they are facing.[191]

***Further Research***

Cyber security is a rapidly evolving issue that is addressed by the First Committee in light of its international peace and security efforts. Moving forward with their research, delegates should consider the following questions: What options are there to bring more clarity to the concepts of cybercrime, cyber warfare, and cyber terrorism? How could capacities be built to identify, prevent, and respond to cyber threats? What role should be played by developed versus developing nations in achieving global cyber security? What hinders international cooperation and which methods can be employed to foster dialogue? What future does the GGE have? How can disagreements be addressed, and compromise reached on issues that are in deadlock while continuing successful work on less contentious areas?

## Annotated Bibliography

Beaver, M. (2016, September 28). The United Nations and Cyberwarfare. *Global Risk Advisors.* Retrieved 20 July 2017 from: https://globalriskadvisors.com/blog/united-nations-cyber-warfare/

*This blog post offers a comprehensive overview of what is commonly understood as cyber warfare, even in the absence of a universally agreed definition, and the involvement of state actors in cyberattacks. It further outlines the efforts of the UN over the last two decades to establish rules and norms regarding global cyber security. Delegates should consult this source to understand the current debate around cyber security and hear a critical voice regarding the UN's capacity to address the issue.*

Brenner, S. (2007). At Light Speed: Attribution and Response to Cybercrime/Terrorism/Warfare. *Journal of Criminal Law and Criminology*, 97 (2): 397-476. Retrieved 29 August 2017 from: http://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=7260&context=jclc

*This journal article takes an academic and at the same time very practical approach to the issue of defining the different concepts of cybercrime versus cyber warfare versus cyber terrorism. It*

[182] Bendiek, Europe's Patchwork Approach to Cyber Defense Needs a Complete Overhaul, *Council on Foreign Relations*, 2017.
[183] Ibid.
[184] Ibid.
[185] WSIS, *WSIS Forum 2017: Information and Knowledge Societies for SDGs – Outcome Document*, 2017.
[186] Ibid.
[187] Maurer, *Cyber Norm Emergence at the United Nations*, 2011.
[188] Ibid.
[189] GIP, Digital Watch, *Digital Policy Trends in June*, 2017; Brenner, *At Light Speed: Attribution and Response to Cybercrime/Terrorism/Warfare*, 2007, pp. 421-424.
[190] Beaver, The United Nations and Cyberwarfare, *Global Risk Advisors*, 2017.
[191] UN DPI, *Half of all countries aware but lacking national plan on cybersecurity, UN agency reports*, 2017.

*presents delegates with possible categories based on which the distinction could be made when it comes to policies. It looks most prominently at the issue of attribution of cyber hostilities as well as the motivation of actors committing cyberattacks. This article helps delegates to understand the difficulty of the issue and may guide them in developing their countries position on the matter.*

Geneva Internet Platform, Digital Watch. (2017). *Digital Watch Observatory* [Website]. Retrieved 30 August 2017 from: https://dig.watch/

*The Digital Watch Observatory of the Geneva Internet Platform is a great resource for delegates to explore various aspects of cyber security. The website offers an overview about cyber norms and various subtopics of cyber security, such as cybercrime, critical infrastructure, and cyberconflict. It also offers policy updates and frequent newsletters that help delegates stay up-to-date on current cyber security concerns and new developments toward the conference. Considering the fast-paced digital landscape, keeping track of the latest cyberattacks, such as WannaCry as well as relevant cyber-events such as WSIS Forum 2017, is very important.*

Geneva Internet Platform, Digital Watch. (2017). *UN GEE* [Website]. Retrieved 20 July 2017 from: https://dig.watch/processes/ungge

*This platform is the perfect source for all essential information on the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. The GGE has published two reports outlining the global cyber security agenda and introducing the principle that international law applies to the digital space. Its work is absolutely crucial for the topic at hand. Tasked with examining cyber threats and making recommendations in this regard, the GGE has not been able to agree on a final report at this point. Delegates should monitor this process closely in the run-up to the conference.*

Radunovic, V. (2015). *Cybersecurity and International Peace and Security.* Retrieved 31 August 2017 from: http://www.gp-digital.org/wp-content/uploads/2015/06/GCCS2015-Webinar-Summary-International-Peace-and-Security.pdf

*This summary on the topic of cyber security and international peace and security provides a concise overview of the issue itself and its importance–including its relevance to human rights–to the international community. It also looks at how it has been addressed so far, by whom, where, and when. This way it helps delegates to build a general understanding of cyber security in the context of the UN General Assembly First Committee's mandate. This source also presents a comprehensive list of mostly regional actors in the field which delegates should research further depending on the regional affiliation of their delegation.*

Tikk-Ringas, E. (2012). *Developments in the Field of Information and Telecommunication in the Context of International Security: Work of the UN First Committee 1998-2012*. Retrieved 20 July 2017 from: http://www.ict4peace.org/wp-content/uploads/2012/08/Eneken-GGE-2012-Brief.pdf

*Although this policy brief published by the ICT4Peace foundation is already 5 years old, it is a great resource to learn how the topic of cyber security has evolved historically within the UN system. It is particularly helpful because it helps delegates to understand the role of the UN General Assembly First Committee in this context and outlines very clearly what the body has been able to do within the boundaries of its mandate and which impediments prevail. Nonetheless, delegates should use this document only as a starting point for their research of the committee's work in more recent years.*

United Nations, General Assembly, Seventy-first session. (2016). *Developments in the field of information and telecommunications in the context of international security (A/RES/71/28)* [Resolution]. Adopted on the report of the First Committee (A/71/445). Retrieved 29 August 2017 from: http://undocs.org/A/RES/71/28

*This resolution is the latest of a series of annual deliberations that the General Assembly First Committee conducts on this topic. The resolution recognizes the importance of ICTs for everyday life and therefore emphasizes the need to ensure its secure usage. From its first proposal in 1998 to 2016, the text has been expanded several times to reflect new developments in the field. Delegates should read this resolution to receive a quick overview what the major concerns of the First Committee are in regards to anything related to cyber and maintaining international peace and security.*

United Nations, International Telecommunication Union. (2017). *Global Cybersecurity Index (GCI) 2017* [Report]. Retrieved 20 July 2017 from: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-R1-PDF-E.pdf

*The Global Cybersecurity Index surveys Member States' commitment to five pillars of cyber security (legal, technical, organizational, capacity building, and cooperation). The 2017 report emphasizes the need for improvement of cooperation at all levels and capacity building which should be a key focus for delegates at the conference. In this report, delegates can also find information specifically regarding their country or region to develop their position for negotiations.*

United Nations, International Telecommunication Union. (2017). *UN Resolutions Related to Cybersecurity* [Website]. Retrieved 20 July 2017 from: http://www.itu.int/en/action/cybersecurity/Pages/un-resolutions.aspx

*This website is a great resource for delegates to research the UN General Assembly's consideration of the topic between 2000 and 2010. Most importantly, it includes resolutions on the global culture of cyber security which discuss the assessment of best practices of cyber security. Delegates should read through all resolutions provided on this website to gain a better understanding of the UN's efforts to enhance cyber security globally specifically through building national capacity.*

United Nations Office for Disarmament Affairs. (2017). *Developments in the field of information and telecommunications in the context of international security* [Website]. Retrieved 20 July 2017 from: https://www.un.org/disarmament/topics/informationsecurity/

*This website offers delegates two important resources. It includes a short synthesis on the GGE process and the prominently discussed topics of "norms, rules or principles of the responsible behavior of states in the cyber sphere as well as confidence-building measures, international cooperation and capacity building." Furthermore, delegates may find their country's submission for the annual reports by the Secretary-General to the General Assembly on "Developments in the field of information and telecommunications in the context of international security."*

## Bibliography


African Union. (2014). *African Union Convention on Cyber Security and Personal Data Protection*. Retrieved 20 July 2017 from: https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf

Beaver, M. (2016, September 28). The United Nations and Cyberwarfare. *Global Risk Advisors*. Retrieved 20 July 2017 from: https://globalriskadvisors.com/blog/united-nations-cyber-warfare/

Bendiek, A. (2017, August 30). Europe's Patchwork Approach to Cyber Defense Needs a Complete Overhaul. *Council on Foreign Relations*. Retrieved 1 September 2017 from: https://www.cfr.org/blog/europes-patchwork-approach-cyber-defense-needs-complete-overhaul

Brenner, S. (2007). At Light Speed: Attribution and Response to Cybercrime/Terrorism/Warfare. *Journal of Criminal Law and Criminology*, 97 (2): 397-476. Retrieved 29 August 2017 from: http://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=7260&context=jclc

CERT India. (2009). *Cyber Security & Role of Cert-In*. Retrieved 1 September 2017 from: https://www.itu.int/ITU-D/cyb/events/2009/hyderabad/docs/rai-role-of-cert-in-sept-09.pdf

Commonwealth Secretariat. (2017). *Commonwealth Cybercrime Initiative* [Website]. Retrieved 1 September 2017 from: http://thecommonwealth.org/commonwealth-cybercrime-initiative

Council of Europe. (2001). *Convention on Cybercrime*. Retrieved 20 July 2017 from: http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm

Council of Europe. (2017). *Chart of signatures and ratifications of Treaty 185*. Retrieved 30 August 2017 from: http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=pgZ8eFeP

Earth Institute & Ericsson. (2016). *ICT & SDGs*. Retrieved 27 September 2017 from: https://www.ericsson.com/assets/local/news/2016/05/ict-sdg.pdf

Fidler, M., & F. Madzingira. (2015, June 22). The African Union Cybersecurity Convention: A Missed Human Rights Opportunity. *Council on Foreign Relations*. Retrieved 30 August 2017 from: https://www.cfr.org/blog/african-union-cybersecurity-convention-missed-human-rights-opportunity

Geneva Internet Platform, Digital Watch. (2017). *Digital Policy Trends in June*. Retrieved 30 August 2017 from: https://dig.watch/sites/default/files/DWnewsletter22.pdf

Geneva Internet Platform, Digital Watch. (2017). *UN GEE* [Website]. Retrieved 20 July 2017 from: https://dig.watch/processes/ungge

Global Cyber Security Capacity Centre. (2017). *Cybersecurity Capacity Portal* [Website]. Retrieved 1 September 2017 from: https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/front

Global Forum on Cyber Expertise (2017, June 8). *Working toward a global cyber capacity building agenda in 2017*. Retrieved 1 September 2017 from: https://www.thegfce.com/news/news/2017/05/31/working-towards-a-global-cyber-capacity-building-agenda-in-2017

Lewis, J. (2002). *Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats*. Retrieved 29 August 2017 from: https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/media/csis/pubs/021101_risks_of_cyberterror.pdf

Lewis, J. (2011). *Confidence-building and international agreement in cybersecurity*. Retrieved 22 October 2017 from: https://citizenlab.ca/cybernorms2012/Lewis2011.pdf

Lewis, J., & G. Neuneck. (2013). *The Cyber Index: International Security Trends and Realities*. Retrieved 30 August 2017 from: http://www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf

Maurer, T. (2011). *Cyber Norm Emergence at the United Nations*. Retrieved 20 July 2017 from: http://www.belfercenter.org/sites/default/files/files/publication/maurer-cyber-norm-dp-2011-11-final.pdf

NATO Cooperative Cyber Defence Centre of Excellence. (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Retrieved 20 July 2017 from: https://www.peacepalacelibrary.nl/ebooks/files/356296245.pdf

NATO Cooperative Cyber Defence Centre of Excellence. (2016, April 04). *OSCE Expands Its List of Confidence-Building Measures For Cyberspace: Common Ground on Critical Infrastructure Protection.* Retrieved 1 September 2017 from: https://ccdcoe.org/osce-expands-its-list-confidence-building-measures-cyberspace-common-ground-critical-infrastructure.html

NATO Cooperative Cyber Defence Centre of Excellence. (2017, July 18). *Geneva Conventions Apply to Cyberspace: No Need for a 'Digital Geneva Convention'*. Retrieved 1 September 2017 from: https://ccdcoe.org/geneva-conventions-apply-cyberspace-no-need-digital-geneva-convention.html

NATO Cooperative Cyber Defence Centre of Excellence. (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Retrieved 29 August 2017 from: https://ccdcoe.org/sites/default/files/documents/CCDCOE_Tallinn_Manual_Onepager_web.pdf

North Atlantic Treaty Organization. (2017). *Cyber defence* [Website]. Retrieved 20 July 2017 from: http://www.nato.int/cps/en/natohq/topics_78170.htm

Radunovic, V. (2015). *Cybersecurity and International Peace and Security.* Retrieved 31 August 2017 from: http://www.gp-digital.org/wp-content/uploads/2015/06/GCCS2015-Webinar-Summary-International-Peace-and-Security.pdf

RAND Corporation. (2017). *Cyber Warfare* [Website]. Retrieved 29 August 2017 from: https://www.rand.org/topics/cyber-warfare.html

Smart, K. (2016, October 7). The UN, Cyberspace and International Peace & Security-Side Event-October 5th. *United Nations Office for Disarmament Affairs.* Retrieved 30 August 2017 from: https://www.un.org/disarmament/update/the-un-cyberspace-and-international-peace-security-side-event-october-5th/

Symantec. (2017). *Internet Security Threat Report 2017*. Retrieved 29 August 2017 from: https://s1.q4cdn.com/585930769/files/doc_downloads/lifelock/ISTR22_Main-FINAL-APR24.pdf

Tikk-Ringas, E. (2012). *Developments in the Field of Information and Telecommunication in the Context of International Security: Work of the UN First Committee 1998-2012*. Retrieved 20 July 2017 from: http://www.ict4peace.org/wp-content/uploads/2012/08/Eneken-GGE-2012-Brief.pdf

United Nations, Counter-Terrorism Implementation Task Force. (2011). *Countering the Use of the Internet for Terrorist Purposes – Legal and Technical Aspects* [Report]. Retrieved 29 August 2017 from: http://www.un.org/en/terrorism/ctitf/pdfs/ctitf_interagency_wg_compendium_legal_technical_aspects_web.pdf

United Nations, Department of Economic and Social Affairs. (2016). *ICTs as a catalyst for sustainable development* [Website]. Retrieved 27 September 2017 from: https://sustainabledevelopment.un.org/index.php?page=view&type=20000&nr=579&menu=2993

United Nations, Department of Economic and Social Affairs. (2017). *Sustainable Development Goal 16* [Website]. Retrieved 22 October 2017 from: https://sustainabledevelopment.un.org/sdg16

United Nations, Department of Public Information. (2017, July 5). *Half of all countries aware but lacking national plan on cybersecurity, UN agency reports* [News Article]. Retrieved 30 August 2017 from: http://www.un.org/apps/news/story.asp?NewsID=57119#.WflAc2iPI2w

United Nations, Department of Public Information. (2017, May 19). *In wake of 'WannaCry' attacks, UN cybersecurity expert discusses Internet safety* [News Article]. Retrieved 29 August 2017 from: http://www.un.org/apps/news/story.asp?NewsID=56796

United Nations, General Assembly, Third session. (1948). *Universal Declaration of Human Rights (A/RES/217 A (III))*. Retrieved 30 August 2017 from: http://www.un.org/en/documents/udhr/

United Nations, General Assembly, Fifty-third session. (1999). *Developments in the field of information and telecommunications in the context of international security (A/RES/53/70)* [Resolution]. Adopted on the report of the First Committee (A/53/576). Retrieved 20 July 2017 from: http://undocs.org/A/RES/53/70

United Nations, General Assembly, Fifty-fifth session. (2001). *Combating the criminal misuse of information technologies (A/RES/55/63)* [Resolution]. Adopted on the report of the Third Committee (A/55/593). Retrieved 20 July 2017 from: http://undocs.org/A/RES/55/63

United Nations, General Assembly, Fifty-seventh session. (2003). *Creation of a global culture of cybersecurity (A/RES/57/239)* [Resolution]. Adopted on the report of the Second Committee (A/57/529/Add. 3). Retrieved 20 July 2017 from: http://undocs.org/A/RES/57/239

United Nations, General Assembly, Fifty-eighth session. (2003). *Developments in the field of information and telecommunications in the context of international security (A/RES/58/32)* [Resolution]. Adopted on the report of the First Committee (A/58/457). Retrieved 20 July 2017 from: http://undocs.org/A/RES/58/32

United Nations, General Assembly, Fifty-eighth session. (2004). *Creation of a global culture of cybersecurity and the protection of critical information infrastructure (A/RES/58/199)* [Resolution]. Adopted on the report of the Second Committee (A/58/481/Add. 2). Retrieved 20 July 2017 from: http://undocs.org/A/RES/58/199

United Nations, General Assembly, Sixty-fourth session. (2010). *Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures (A/RES/64/211)* [Resolution]. Adopted on the report of the Second Committee (A/64/422/Add. 3). Retrieved 20 July 2017 from: http://undocs.org/A/RES/64/211

United Nations, General Assembly, Sixty-fifth session. (2010). *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (A/65/201)*. Retrieved 1 September 2017 from: http://www.undocs.org/A/65/201

United Nations, General Assembly, Seventieth session. (2015). *Developments in the field of information and telecommunications in the context of international security (A/RES/70/237)* [Resolution]. Adopted on the report of the First Committee (A/58/457). Retrieved 20 July 2017 from: http://undocs.org/A/RES/70/237

United Nations, General Assembly, Seventy-first session. (2016). *Confidence-building measures in the regional and subregional context (A/RES/71/39)* [Resolution]. Adopted on the report of the First Committee (A/71/450). Retrieved 1 September 2017 from: http://undocs.org/A/RES/71/39

United Nations, General Assembly, Seventy-first session. (2016). *Developments in the field of information and telecommunications in the context of international security (A/RES/71/28)* [Resolution]. Adopted on the report of the First Committee (A/71/445). Retrieved 29 August 2017 from: http://undocs.org/A/RES/71/28

United Nations, General Assembly, Seventy-first session. (2016). *Developments in the field of information and telecommunications in the context of international security – Report of the Secretary-General (A/71/172)*. Retrieved 20 July 2017 from: http://undocs.org/A/71/172

United Nations Institute for Disarmament Research. (2016). *Report of the International Security Cyber Issues Workshop Series*. Retrieved 20 July 2017 from: http://unidir.org/files/publications/pdfs/report-of-the-international-security-cyber-issues-workshop-series-en-656.pdf

United Nations Institute for Disarmament Research. (2017). *Cyber* [Website]. Retrieved 31 August 2017 from: http://www.unidir.org/est-cyber

United Nations, International Telecommunication Union. (2007). *Global Cybersecurity Agenda (GCA).* Retrieved 31 August 2017 from: https://www.itu.int/en/action/cybersecurity/Documents/gca-chairman-report.pdf

United Nations, International Telecommunication Union. (2014). *Understanding cybercrime: Phenomena, Challenges and Legal Response* [Report]. Retrieved 30 August 2017 from: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Cybercrime2014_E.pdf

United Nations, International Telecommunication Union. (2017). *Global Cybersecurity Index (GCI) 2017* [Report]. Retrieved 20 July 2017 from: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-R1-PDF-E.pdf

United Nations, International Telecommunication Union. (2017). *ITU Cybersecurity Activities* [Website]. Retrieved 31 August 2017 from: https://www.itu.int/en/action/cybersecurity/Pages/default.aspx

United Nations, International Telecommunication Union. (2017). *ITU-EC-ACP Project* [Website]. Retrieved 1 September 2017 from: https://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/Pages/default.aspx

United Nations, International Telecommunication Union. (2017). *Regional Cybersecurity Centres.* [Website]. Retrieved 31 August 2017 from: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Regional_Cybersecurity_Centre.aspx

United Nations, International Telecommunication Union. (2017). *UN Resolutions Related to Cybersecurity* [Website]. Retrieved 20 July 2017 from: http://www.itu.int/en/action/cybersecurity/Pages/un-resolutions.aspx

United Nations Office for Disarmament Affairs. (2015). *Developments in the field of information and telecommunications in the context of international security* [Fact Sheet]. Retrieved 30 August 2017 from: https://unoda-web.s3-accelerate.amazonaws.com/wp-content/uploads/2015/07/Information-Security-Fact-Sheet-July2015.pdf

United Nations Office for Disarmament Affairs. (2017). *Developments in the field of information and telecommunications in the context of international security* [Website]. Retrieved 20 July 2017 from: https://www.un.org/disarmament/topics/informationsecurity/

United Nations Office for Disarmament Affairs. (2017). *Military Confidence-building* [Website]. Retrieved 30 August 2017 from: https://www.un.org/disarmament/cbms/

World Summit on the Information Society. (2017). *WSIS Forum 2017: Information and Knowledge Societies for SDGs – Outcome Document.* Retrieved 30 August 2017 from: https://www.itu.int/en/itu-wsis/Documents/wf17/WSISForum2017_ForumTrackOutcomes.pdf