ICT4PEACE NORMS PROJECT
DRAFT WORKING PAPER

NORMS FOR INTERNATIONAL PEACE AND SECURITY:
THE NORMATIVE FRAMEWORKS OF INTERNATIONAL CYBER COOPERATION

Mika Kerttunen (Editor)
Saskia Kiisel (Co-editor)

April 2015

The ICT4Peace Norms Project

The ICT4Peace Norms project is intended to build on the work and views of international experts, analyzing what guides state actions in cyberspace. The project seeks to identify accepted practices in, and common and prospective interpretations of, international cyber security-related norms.

Topics covered by the project include: the public expectation to be protected against malicious cyber activities; international cooperation in the field of cyber security; the balance between privacy, freedom of information and national security; issues relating to subversion and espionage; ways to support multi-stakeholder decision-making; and the role of the private sector in international cyber security.

The ICT4Peace norms working group has invited and received contributions from a wide range of international scholars and experts. In particular, we note and appreciate the materials, notes, views and time of Prof. Catherine Lotrionte, Mr. Christopher Spirito, Dr. Anatoly Streltsov, Dr. Mika Kerttunen, Dr. Jarno Limnell, Mr. Jerome Uchenna Orji, Dr. Elaine Korzak, Dr. Eneken Tikk-Ringas, Mr. Zahid Jamil, Mr. Rafal Rohozinski, Dr. Adamantia Rachovitza, Dr. Paul Cornish, Mr. Jens Kremer, Dr. Roger Hurwitz, Dr. Panayotis Yannakogeorgos, Dr. William Boothby, Prof. Daniel Ryan, Dr. Nils Melzer, Dr. Tughral Yamin, Dr. Kim So Jeong, Mr. Alexey Yankovski and Ms. Lisette den Breems. We are indebted to Ms. Liisi Adamson, Ms. Agnes Zaure, Ms. Saskia Kiisel and Mr. Kristjan Kikerpill for their research and outreach support as well the editorial work on the draft working papers.

The papers produced in the course of this Norms Project do not reflect individual views or conclusions of any one contributor but seek to include a variety of views and proposals to be considered in further thinking about international law and responsible state behavior.

The present reports are works in progress, and will be revised in light of further comments and suggestions collected during the GCCS and subsequent interviews. In particular, the work will be presented and discussed at a high-level panel during GCCS Conference in The Hague, Netherland, the results of which will be reflected in the final papers.

The ICT4Peace Foundation's is deeply grateful for the substantive and financial support provided by the Ministry of Foreign Affairs of the Netherlands and Microsoft to the current phase of the project. A special thank goes to Ms. Lisette den Breems of the Ministry of Foreign Affairs, The Netherlands, for her important substantive support. The project is led by Dr. Eneken Tikk-Ringas (IISS) who has been directing the ICT4Peace's work on norms since 2012 in her capacity as Senior Advisor to the ICT4Peace Foundation. ICT4Peace is committed to continuing this work beyond the Hague Conference with current and new partners interested in exploring this challenging and important topic.

THE NORMATIVE FRAMEWORKS OF INTERNATIONAL CYBER COOPERATION

The need and purpose of cooperation on cyber security issues is emphasised in the UN Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security report to the General Assembly as follows:

> "Member States have frequently affirmed the need for cooperative action against threats resulting from the malicious use of ICTs. International cooperation is essential to reduce risk and enhance security. Further progress in cooperation at the international level will require actions to promote a peaceful, secure, open and cooperative ICT environment. Cooperative measures that could enhance stability and security include norms, rules and principles of responsible behaviour by States, voluntary measures to increase transparency, confidence and trust among States and capacity-building measures. States must lead in these efforts, but effective cooperation would benefit from the appropriate participation of the private sector and civil society."[1]

Cyberspace and its issues, solutions as well as threats, do not obey or recognize territorial or organisational borders - the political lines of demarcation drawn to control our daily life on the planet. No single national or international entity has the intellectual, financial or material resources to design, operate and maintain its level of ambition, development and operation alone. Due to the nature of cyberspace even the strongest of states need to cooperate. The United States' international cyber strategy emphasises this requirement by contrasting working together with succumbing "to narrow interests and undue fears".[2]

The following analysis looks into the existing political and legal mechanisms for cooperation aimed at an open, resilient, secure and peaceful cyberspace. It asks how and in which aspects states already do cooperate in the absence of one uniform legal norm, while in accordance with the existing international law and responsible attitude towards shared or perceived threats. The following, more precise, questions reveal the focus of the study:

> (i) How is international cooperation, more specifically cyber operations, mandated by national and international statues, treaties or other regulatory instruments;
>
> (ii) What political, legal and other normative debates are taking place regarding international cooperation and cyber cooperation;

Before the normative examination, the paper begins with an analysis of the central notions of norm, and cooperation. Here, the foundations, assumptions and boundaries of these concepts are examined in order to better link on-going conceptual discussion to the practical challenges in normative considerations. Specific attention is paid to confidence building measures a particular form of cooperation and a norm.

---

[1] UN General Assembly, "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security: Note by the Secretary-General", A/68/98, 24 June 2013.

[2] The White House, *International Strategy for Cyberspace*, May 2011,

The account takes a dualist view where general normative goals or norms are set for international cooperation, these are to be implemented in good faith and to the highest benefit of their addressees, but recognizing that states do also tend to follow egoistic strategies. Another important point-of-departure is that implementation of international law and its principles materialising in regional and national normative processes and instruments. Thus, indicative of what states have accepted as their standards of behaviour guided by international law, whether their national laws supporting relevant concepts and goals

Theoretical Observations: Norms and Cooperation

Norms in international law generally refer to binding obligations between states. In international relations and diplomacy, a norm stands for a standard of appropriate behaviour for actors with a given identity.[3] Paying attention to the foundations of norms asks important question about the origin, shape and focus of norms: who creates them, to whom or what they apply to, how do they function or how are they governed and what are the ideational patterns and values behind the collective expectations. Therefore, norms as well as other, more precise, normative instruments are mobile and subject to debate as well as internal and external marketing and exchange. Norms and regulations as artefacts and products of exchange apply in particular to international relations and cooperation where different values, practices, political and legal systems meet.

Cooperation can be defined as actors adjusting "their behaviour to the actual or anticipated preferences of others, through a process of policy coordination".[4] Cooperation can also be viewed as an exchange of values where the individual calculations and expectations condition the play between the engaged actors. This view pays attention to the rewards, profits and non-profits as well as the frequency and durability of the [cooperative] relationship.[5] What sustainable cooperation thus requires is that the involved actors firstly, at some minimal level, acknowledge and share similar goals and secondly gain rewards.[6] This expectation raises two main challenges: who defines the goals and how are the rewards gained and distributed among the participants. The latter also implicitly refers to the distribution of costs of cooperation.

In addition to the explanations of shared goals, frequent threats, and expected gains, genuine cooperation is expected to occur when:

- The number of participants is relatively low; whereas larger number of participants would increase the opportunities of interaction and gains;
- The participants believe in continuing to interact with each other for a long or indefinite period of time; i.e. trust, often a rare commodity in politically,

[3] Martha Finnemore and Kathryn Sikkink, 'International Norm Dynamics and Political Change', *International Organization*, vol. 52, no. 4, Autumn 1998, p. 891. Also Peter J Katzenstein, *The Culture of National Security. Norms and Identity in World Politics* (New York: Columbia University Press, 1996).

[4] Robert Keohane, *After Hegemony* (Princeton: Princeton university Press, 1984), fn. 1; originally in Charles Lindblom, *The Intelligence of Democracy* (New York: Free Presss, 1965), p. 227.

[5] Robert Axelrod, *The Evolution of Cooperation* (New York: Basic Books, 1984).

[6] Helen Milner, "International Theories of Cooperation among Nations. Strengths and Weaknesses", *World Politics* 44 (April 1992), pp. 466-496.

intellectually, financially or militarily sensitive areas, would increase because of repeated positive exchanges;
- International regimes, organizations or other external actors facilitate cooperation;
- Epistemic, expert communities speak in favour of cooperation;
- Asymmetry of power and capability exist, allowing the stronger actors to have more dominant roles while enabling the weaker ones to excel in niche capabilities and receive absolute gains.[7]

The enforcement school of international cooperation theory points that a key problem in international cooperation is states possessing incentives to violate international agreements. However, the managerialists do not regard monitoring, sanctioning or suspension mechanisms essential to maintaining cooperation, but pay attention to the complexity and ambiguity of cooperation problems, for example, to the lack of clarity and priorities.[8]

Seen through a general framework of international theories of cooperation, cyber as a field possesses a number of catalytic characteristics. Cyberspace is borderless - its systems, functions as well as threats are interconnected – and thus shared. Practically the whole epistemic community speaks for cooperation, enabling the mightier and lesser nations to find their specific roles. Cooperation should constitute a rule rather than an exception. However, as cyber vulnerabilities and capabilities are often sensitive in nature, dealing with political, military or commercial interests, the necessary trust and courage to reveal one´s true state of affairs is often lacking. Due to the notion that cyber as a policy area is relatively new there are few established fora, developed patterns or generalized experiences to build on. Yet in *terra incognita*, cooperation is or should be more actively sought after in than within well-known areas. Cooperation creates trust, durability and expectancy of profits, and within cyber security there are several important areas to cooperate in and proceed from.

The UN General Assembly Resolution 57/239 (2002) on the Creation of a Global Culture of Cybersecurity as well as UN Resolution 58/199 (2003) on the Creation of a Global Culture of Cybersecurity and the Protection of Critical Information Infrastructures recognised the need for a high level of cyber security as governments, businesses, organisations and individuals have become dependent on information technologies. Moreover, the 2002 Resolution noted interconnectivity, information systems and networks becoming exposed to a wider variety of threats and vulnerabilities. The Resolution also called for participants "to prevent, detect and respond to security incidents in a timely and cooperative manner". This entailed sharing of information and implementing procedures for "rapid and effective cooperation", including cross-border information-sharing and cooperation.[9]

---

[7] Milner, following mainly Axelrod, Grieco, Haas, Keohane, and Krasner, pp. 470-480.
[8]Johannes Urpelainen, "Enforcement and capacity building in international cooperation", *International Theory* (2010), 2:1, pp. 32–49. Urpelainen draws his enforcement account mainly from Carrubba, Downs, Gilligan, and Keohane and the managerial interpretation from Chayes and Chayes, Mitchell, Tallberg, and Young.
[9] United Nations Resolution on Creation of a Global Cybersecurity Culture, A/RES/57/239 (20 December 2002); United Nations Resolution on Creation of a Global Cybersecurity Culture and the Protection of Critical Information Infrastructure, A/RES/58/199 (23 December 2003).

However, the abovementioned contextual factors and declaratory and legally non-binding notes determine neither cooperation nor its outcome. Politicians and states always try to calculate and balance between competing needs and available options. Cooperation that does not restrain itself to traditional political and organizational boundaries, albeit in a new policy area, is easily resisted. As all politics is local domestic political considerations, requirements to allocate resources to more urgent and politically more tangible policies and projects can strike through cyber security investments. Although nations and societies are dependent on functioning information systems, their structural, functional and ambition levels within cyberspace differ. Last but not least, established administrative and bureaucratic patterns, i.e. turf wars between national authorities such as different ministries as well as international agencies and organizations, e.g. ministries for foreign affairs, telecommunication, and commerce or NATO and the EU, can inhibit cooperation otherwise appearing rational.

Content analysis of international cyber security instruments reveals a list of categories and types of cooperation: there are different means to achieve shared goals in case of cyber security. Pursuant to the main international organizations' instruments, cooperation may take the form of sharing (of information, data, intelligence, best practices, contacts, expertise etc.). This form of cooperation generally follows from a voluntary decision or a politically agreed framework (e.g. OSCE Confidence Building Measures) and normally, at minimum, requires extending already existing resources or routines to cooperation partners' interests and requirements. Cooperation can also take the form of assistance, the language used in e.g. 1949 Washington Treaty establishing the North Atlantic Alliance. Assistance can occur in various contexts, such as a response to a threat or providing human, financial or material resources lacking at the requesting/receiving end. Compared to sharing, assistance may require allocation of extra resources and procedures to provide the other party with expected contribution in order to reach a mutually expected or desired outcome. Assistance is a widely used term in the context of law enforcement cooperation.[10] Finally, assistance can be requested and provided to non-state entities as well, for example in the case of the NATO Industry Cyber Partnership initiative.

As cooperation is content-specific and –conditioned, even explicit normative direction remains subject to contingent interpretation. For example, in the absence of clarity in international law, and building on the spirit of it, it remains up to countries to additionally take national measures of cooperation, such as *inter alia* advising their agencies to cooperate in specific cases or clearly stipulate the mandate of a national CERT with provisions on cooperation.

Cyber cooperation mandates

The most prominent areas and contexts of cyber security cooperation arguably consists of collective peace and security; national defence; national security and crisis management; law enforcement and crime; and routine awareness, prevention and mitigation mechanisms

[10] In addition to the network of informal bilateral relationships between law enforcement agencies, INTERPOL maintains a system of national central bureaus in 190 countries. Bureaus are typically designated sections with the national law enforcement agency. Through an online 'I-24/7' system, bureaus may facilitate either bilateral or multilateral informal police-to-police requests, or the transmission of a formal mutual legal assistance request from one central authority to another – via the national central bureaus."

(such as CERT cooperation). Within each of the mentioned fields one can distinguish specific forms and methods of cooperation in e.g. capacity building or capability development but for the purpose of this chapter, such analysis is only relevant from specific normative, regulative perspectives. The international legal framework for cooperation needs to be supported by national provisions.

The basis for international peace and security cooperation derives from the UN Charter and regional security treaties that entail numerous norms that require cooperation in different fields at various occasions.[11] The UN Charter speaks of collective measures as well as harmonizing actions of nations in its first article:

> *The Purposes of the United Nations are:*
> *1. To maintain international peace and security, and to that end: to take effective collective measures for the prevention and removal of threats to the peace, and for the suppression of acts of aggression or other breaches of the peace, and to bring about by peaceful means, and in conformity with the principles of justice and international law, adjustment or settlement of international disputes or situations which might lead to a breach of the peace;*
> *2. To develop friendly relations among nations based on respect for the principle of equal rights and self-determination of peoples, and to take other appropriate measures to strengthen universal peace;*
> *3. To achieve international co-operation in solving international problems of an economic, social, cultural, or humanitarian character, and in promoting and encouraging respect for human rights and for fundamental freedoms for all without distinction as to race, sex, language, or religion; and*
> *4. To be a centre for harmonizing the actions of nations in the attainment of these common ends.*

In their wording, the Charter and majority of the regional treaties are not limited to any particular type of threat and therefore are also applicable to cyber security, provided that relevant thresholds and procedural conditions are met. This stand thus constitutes the legal basis for cyber cooperation between alliances or individual countries. However, international peace and security cooperation can extend beyond defence and military security issues and the principal legal basis for such cooperation can be derived from the legal obligation of peaceful settlement of disputes,[12] which is considered a customary law norm[13] and a foundation stone of rule of law in international relations.[14] According to Simma *et al*. peaceful settlement of disputes suggests that States are under an obligation to deploy active efforts for the settlement of their international disputes.[15] Therefore, Article

[11] For example see NATO, OSCE Charter on Preventing and Combating Terrorism, African Union Convention on Cyber Security and Personal Data Protection, ASEAN 2004 Vietiane Action Programme 2004-2010, SCO Agreement between the governments of the member states of the Shanghai Cooperation Organisation on cooperation in the field of the international information security etc.
[12] Katharina Ziolkowski (ed.), *Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy* (Tallinn: CCD COE Publishing, 2013), p. 175.
[13] ICJ 27.06.1986. Paramilitary Activities in and against Nicaragua (*Nicaragua v. United States of America*), para 290.
[14] Bruno Simma, Daniel-Erasmus Khan, Georg Nolte, Andreas Paulus (eds). *The Charter of the United Nations. A Commentary*. 3rd Edition, Volume I, (Oxford: Oxford University Press 2012), p.187.
[15] *Ibid*, p. 190.

2(3) of the UN Charter can be regarded as a variation of the duty to cooperate as according to it "All Members shall settle their international disputes by peaceful means in such a manner that international peace and security, and justice, are not endangered." This does not constitute a positive obligation, but offers a normative and customary law based platform for consensus building. Accordingly, the Friendly Relations Declaration provides that 'States shall […] seek early and just settlement of their international disputes'[16] and the Manila Declaration supplements to the formula by adding the phrase 'in good faith and in a spirit of co-operation'.[17] Moreover, the Friendly Relations Declaration explicitly states that '[…] States shall co-operate with other States in the maintenance of international peace and security […].'[18]

More specifically, and following Ziolkowski, it can be argued that the duty of states to cooperate has a normative binding character whenever it is endorsed in international treaties establishing and governing international organisations. Albeit the large body of indications and empirical examples, the notion and normative character of a general duty to cooperate is disputed among scholars.[19] Nevertheless, given the universality of the UN Charter and the importance of the Friendly Relations Declaration, nearly all States have taken a conventional obligation to cooperate, which would thus also apply in the realm of cyberspace as far as it supports the maintenance of international peace and security.[20]

Even though there is no unified legally binding norm that would unequivocally establish an obligation for States to cooperate, there are several norms that require cooperation in different forms, different fields and at various occasions. For example, in international law enforcement cooperation the nature of criminal law itself sets demands for a solid legal basis. Today's cross-border nature of crime relies on inter-State cooperation, an approach that has been long recognized by States.[21] Due to the expectation of just procedure and the presumption of innocence, it is essential that the gathering of evidence and the exchange of relevant information follow an established legal pattern. Indeed, cooperation in criminal investigations cannot be justified without a binding multilateral or bilateral agreement between parties in question. Types and forms of security cooperation are generally are loosely regulated, primarily for contingent political and administrative purposes, with the main emphasis on expected benefits and shared goals of the cooperation.

A relatively new form of cooperation making a great impact on cyber security is cooperation between CERTs and other computer emergency response mechanisms. For this type of cooperation, little international or, for that matter, even bilateral legal basis can be identified. However, it follows from the purpose and national mandates of CERTs that the exchange of information and mutual provision of assistance is at the core of their functions

---

[16] UN General Assembly A/RES/25/2625. *Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations*. Adopted 24 October 1970, para 2.
[17] UN General Assembly. A/RES/37/10. *Manila Declaration on the Peaceful Settlement of International Disputes*. Adopted 15 November 1982. Chapter I, para 5.
[18] Friendly Relations Declaration, Principle 4 *The duty of States to co-operate with one another in accordance with the Charter.*
[19] Katharina Ziolkowski (ed.), *Peacetime Regime for State Activities in Cyberspace*, p. 176.
[20] Katharina Ziolkowski, *Confidence Building Measures for Cyberspace – Legal Implications*, NATO CCD COE, 2013, p. 79.
[21] See for example Budapest Convention or Prüm Treaty.

and thus does not, *per se*, require a separate agreement between collaborating entities or a treaty.

In her 2011 "Ten Rules of Cyber Security", Tikk-Ringas has offered one of the few normative approaches to cyber cooperation. In the aftermath of the Estonia 2007 cyberattacks and from a state security perspective, she considered cyber conflict as a breach of internal policies and regulations as well as legal obligations. By default, it thus represented an infringement on regulated and expected responsible, non-harmful state behaviour. Within this framework, the levels and sources of regulatory instruments cover standards, best practices, contracts, internal explicit regulations and national and international agreements and customary law. More explicitly, Tikk-Ringas argues [as a rule of a specific duty to cooperate] that:

> "The fact that a cyberattack has been conducted via information systems located in a state's territory creates a duty to cooperate with the victim state."

Of the normative foundations of cooperation, Tikk-Ringas mentions the 2001 Convention on Cybercrime inviting the parties to cooperate through the application of relevant international instruments, arrangements agreed to by uniform or reciprocal legislation and domestic laws. Normative expectation of cooperation is also coded in the 1949 North Atlantic Treaty, calling for the Alliance nations to consult whenever any nation regards its territorial integrity, political independence or security as being threatened. Furthermore, the rule of mandate, stating that an "organisation's capacity to act (and regulate) derives from its mandate" forwards an obvious but frequently neglected approach to international relations where regulatory instruments operate as well. An earlier analysis of legal and policy instruments had revealed the overlaps and gaps in international coordination and harmonization.[22]

Cooperation as an explicit or implicit norm raises the question of responsible state behaviour and its normative and political grounds. In 2013, the UN Group of Governmental Experts [GGE] on Developments in the Field of Information and Telecommunications in the Context of International Security agreed on a set of norms concerning appropriate state behaviour, that is, of the applicability of international law to ICT-related activities in armed conflict as well as outside of the context of armed conflict, e.g. principles of sovereignty and state responsibility. GGE also went on to discuss measures aimed at promoting responsible state behaviour regarding the use of proxies; the principles for applying non-forcible counter-measures; and measures to promote responsible state behaviour in particular below the threshold activities that are potentially destabilizing.[23] Regarding cybersecurity, states have not agreed on robust confidence building measures that would set restrictive normative regulations on their behaviour in cyberspace.

The third GGE (2013) managed to break important ground in the international cybersecurity dialogue, recognising that the application of norms derived from existing

---

[22] Eneken Tikk, "Ten Rules of Cyber Security", *Survival*, vol. 53, no. 3, June-July 2011, pp. 119-132; Eneken Tikk, *Frameworks for International Cyber Security: Law and Policy Instruments* (Tallinn: CCD COE Publishing, 2010).

[23] See for example Michele Markoff, "Remarks", at the First Committee Thematic Discussion on Other Disarmament Issues and International Security, New York, NY, October 30, 2013 at http://usun.state.gov/briefing/statements/216133.htm.

international law relevant to the use of ICTs by States is essential in order to reduce risks concerning international peace, security and stability and listing a number of norms applicable in this context.[24] The group emphasised a noticeable increase in risk as ICTs are used for crime and the conduct of disruptive activities and acknowledged the need for common understandings on norms, rules and principles applicable to the use of ICTs by States as well as voluntary confidence-building measures to advance peace and security.[25]

In 2013, the GGE concluded that international law was applicable in and to cyberspace: [19.] "International law, and in particular the Charter of the United Nations, is applicable and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT environment." Moreover the GGE stated that [22.] "States should intensify cooperation against criminal or terrorist use of ICTs, harmonize legal approaches as appropriate and strengthen practical collaboration between respective law enforcement and prosecutorial agencies."[26]

The third GGE also resulted in a consensus report and acknowledged the need to separate the questions where the UN First Committee would have greater weight and legitimacy among the international community from the broader issues of cybersecurity, which would essentially allow them to add a substantive layer to the work done in other forums.

The 2013 GGE agreed that practical transparency and CBMs, such as high-level communication and timely information sharing, could enhance trust and assurance among states and help reduce the risk of conflict by increasing predictability and reducing misperception. The Group agreed on the vital importance of capacity building to enhance global cooperation in securing cyberspace. The Group reaffirmed the importance of an open and accessible cyberspace, as it enables economic and social development. And, the Group agreed that the combination of all these efforts support a more secure cyberspace.[27]

Confidence-building measures can be seen as a particular form of politically binding norm focusing on cooperative and responsible state behaviour to maintain international peace and security. In general, CBMs are aimed at mitigating political tensions, mistrust and preventing (the danger of) war.[28] Transparency of activities would diminish suspicion and increase confidence, it is believed. The measures include annual exchange of information of defence planning and activities, in particular about expenditure, acquisition and major exercises. Specified units, facilities and exercises can be opened to verification and monitoring. CBMS are considered necessary to enhance predictability and reduce the prospect that misattribution or misperception might mistakenly lead to conflict.

---

[24] UN General Assembly, "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security: Note by the Secretary-General', A/68/98, 24 June 2013.
[25] Ibid, p. 6.
[26] Ibid, p. 8.
[27] UN General Assembly, "Group of Governmental Experts on Developments in the Field of Information and Telecommunications"; see also Markoff, (2013), "Remarks".
[28] See, e.g. UN Department of Political and Security Council Affairs, *Comprehensive Study of Confidence-Building Measures* (New York: United Nations, 1982), para 16, http://www.un.org/disarmament/HomePage/ODAPublications/DisarmamentStudySeries/PDF/SS-7.pdf.

Most of the underlying assumptions regarding CBMs apply to cyberspace, too. Thus, cooperative cyber-CBMs could consist of measures such as transparency and communication measures of publicising cyber security strategies, communicating military strategies, displaying the organisational structures of national and military CERTs, and exchanging contact information between agreed points of contact as well as exposing units and exercises for verification. Exchanges of military curricula, joint training and exercises would also be beneficial as they present indications about military thinking and capabilities. Moreover, cooperative measures could consist of mutual aid, CERT data sharing and incident response, technical assistance in forms of best practices and information assurance. Another very practical and important set of CBMs are stability and restraint measures in which parties agree to limit, criminalise or exclude certain de-stabilising and offensive measures. Given the on-going development in the field of autonomous cyber warfare capabilities, cyber CBMs or a regime limiting the targeting of critical services or infrastructure as well as the exclusion of cyber offensive measures would be most valuable to increasing predictability and thus security and stability.[29]

Western, predominately European approaches to cooperation consist of few hard law instruments such as EU Directives and bilateral agreements accompanied with a number of soft law instruments such as strategies, communiqués and recommendations. According to Renard, between the European Union and its strategic partners, two kinds of bilateral agreements facilitate cooperation against cybercrime. Firstly, legal acts related to cooperation on law enforcement and, for example, the agreements on extradition and mutual legal assistance - deemed important because they facilitate cooperation in the course of (cyber-) criminal investigations - fall under this category. Mutual legal assistance also facilitates the setting up of joint investigations teams. Renard also notes that for example the 2003 EU-US agreements offer a framework for cooperation, but they nonetheless co-exist with bilateral agreements between the US and EU member states. The 2009 EU-Japan mutual legal assistance agreement, on the other hand, is a self-standing accord, making up for the absence of bilateral agreements with EU member states.[30]

Secondly, there are agreements that allow for exchanges and cooperation between operational agencies.[31] These agreements have been described as a 'sub-category' of bilateral agreements, including agreements concluded between EU agencies and partner countries. The number of such agreements has been steadily increasing, but their scope remains limited. The nature of the cooperation agreements can vary, ranging from

---

[29] Daniel Stauffacher and Camino Kavanagh, *Confidence Building Measures and International Cyber Security* (Geneva: ICT4Peace Foundation, 2013), pp. 6–12, http://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/ICT4Peace%20-%20International%20Dialogue%20on%20CBMs%20and%20International%20Cyber%20Security.pdf; also *The Role of CBMs in Assuring Cyber Stability*, UNIDIR Cyber Security Conference 2012 (CS12), http://www.unidir.org/files/publications/pdfs/the-role-of-cbms-in-assuring-cyber-stability-fr-384.pdf. Some sources use interchangeably the terms of CBM and CSBM, confidence and security building measures.

[30] Thomas Renard, "The rise of cyber-diplomacy: the EU, its strategic partners and cyber-security", *European Strategic Partnership Observatory*, Working Paper no. 7, 2014.

[31] The EU Justice and Home Affairs council adopted the Council decision of 27 March 2000 (amended by Council Decision of 7 December 2001 and the Council Decision of 13 June 2002), which authorises the Director of Europol to enter into negotiation on cooperation agreements with third States and non-EU related bodies. See further Europol. External Cooperation. Available at: https://www.europol.europa.eu/content/page/external-cooperation-31.

operational cooperation, including the exchange of personal data, to technical or strategic cooperation. Europol has concluded an operational agreement with twelve countries, including Canada and the US, enabling the EU and its partners to share highly sensitive information.[32] Europol has also concluded six 'strategic agreements', for example with Russia, that however, do not offer the same level of confidentiality, thus inhibiting the exchange of sensitive data. In 2009, the Council of the EU mandated Europol to start negotiating an operational agreement with Russia to further cooperation, although the ultimate conclusion of this agreement remains difficult.[33]

In addition to such EU-wide as well as international instruments, a number of multilateral organisations have proven their value in developing or coordinating cybersecurity policies with the EU. In the framework of the UNODC expert group on cybercrime, the EU and the US regularly coordinate their respective positions. The Group of Eight has also been active in cybersecurity, setting up a sub-group on high-tech crime in which the EU is an observer. The EU has actively supported the establishment of confidence-building measures with Russia in the framework of the OSCE, and with China and other Asian countries in the framework of the ASEAN Regional Forum. The London Process convening international leaders annually to generate a consensus on responsible behaviour in cyberspace, is another cooperative platform for discussing cyber issues. With NATO, the EU has conducted informal staff talks on cyber security including cybersecurity awareness, joint trainings, and developing capabilities in terms of cyber-resilience.[34]

The EU Cybersecurity Strategy prioritises the EU's international cyberspace policy in terms of freedom and openness, outlining the vision and principles of EU core values and fundamental rights in cyberspace. The emphasis on cybersecurity capacity building entails from the EU the willingness to engage with international partners, the private sector and civil society to support capacity building in third countries. The strategy also aims to foster international cooperation in cyberspace issues, with the goal of preserving an open, free and secure cyberspace. This is viewed as a global challenge the EU is addressing together with relevant international partners and organisations as well as the private sector and civil society.[35]

The proposed EU Directive on Network and Information Security requires Member States to increase their preparedness and improve their cooperation with each other in the areas of critical infrastructures of energy, transport, information society services, public administrations etc. Additionally, it requires Members States to adopt appropriate measures to manage security risks and incidents reporting. The proposed Directive also aims at creating a collaboration framework, within which the Member States and the European Commission can share early warnings about risks and incidents. It also foresees a role for ENISA in terms of facilitating collaboration and managing security risks and information with Member States. Furthermore, the proposed Directive helps to establish common minimum requirements for network and information security at the national level.

---

[32] Europol has operational agreements with the US, Monaco, Liechtenstein, Switzerland, Serbia, Norway, Iceland, Former Yugoslav Republic of Macedonia, Colombia, Canada, Australia, Albania.
[33] Renard, "The rise of cyber-diplomacy.
[34] Ibid.
[35] Joint communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on a Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, Join (2013).

It requires Member States to designate national competent authorities for NIS, and draw up strategies on network and information security supported by the operation of CERTs' risk mitigation and response mechanisms. It is also expected that the private sector will develop its own cyber resilience capacities and shares best practices across sectors.[36]

The Council of Europe's Convention on Cybercrime is the only legally binding international agreement on cybersecurity, focusing on cybercrime. The Convention principally aims at harmonising the substantive domestic criminal law elements of offences and connected provisions in the area of cybercrime; providing for domestic criminal procedural law the powers necessary for the investigation and prosecution of such offences as well as other offences committed by means of a computer system or gathering evidence in electronic form related to the aforementioned crimes; as well as setting up a fast and effective regime of international co-operation.[37] Article 23 sets forth three general principles with respect to international co-operation:

1) Firstly, international co-operation is to be provided among Parties "to the widest extent possible." This principle requires Parties to provide extensive cooperative measures to each other, and intends to minimise impediments to the smooth and rapid flow of information and evidence internationally;
2) Secondly, cooperation is to be extended to all criminal offences related to computer systems and data; and
3) Cooperation is to be carried out both "in accordance with the provisions of this Chapter" and "through application of relevant international agreements on international co-operation in criminal matters, arrangements agreed to on the basis of uniform or reciprocal legislation, and domestic laws."[38]

The 2010 revision of the NATO Policy on Cyber Defense defines cyber threats as a potential source for collective defence in accordance with Article 5 of the Washington Treaty and collective defence response is subject to the decision of the North Atlantic Council. Cyber defence measures are incorporated and integrated across all Alliance missions, yet the Alliance has emphasised not engaging in offensive cyber capability development and operations.

In accordance of Article 5 of North Atlantic Treaty NATO nations will provide coordinated assistance if an Ally or Allies suffer a cyberattack. To achieve this, NATO will enhance consultation mechanisms, early warning, situational awareness and information sharing among the Allies. To facilitate these activities, NATO has a framework of cyber defence Memoranda of Understanding in place between the Allies' national cyber defence authorities and the NATO Cyber Defence Management Board.

In the Wales 2014 Summit Declaration NATO reaffirmed the Enhanced Cyber Defence Policy principles of the indivisibility of Allied security and of prevention, detection, resilience, recovery, and defence. Moreover, the Summit reminded that NATO cyber policy recognises that international law, including international humanitarian law and the UN Charter, applies in cyberspace. NATO Nations committed to continue actively engaging on cyber issues with relevant partner nations on a case-by-case basis and with other international organisations,

[36] European Union Agency for Network and Information Security (ENISA), *Cybersecurity Cooperation*, October 2013.
[37] Convention of Cybercrime, Budapest, 23 November 2001, Explanatory Report.
[38] Convention of Cybercrime, Budapest, Article 23.

including the EU, as agreed upon, as well as to intensify cooperation with industry through a NATO Industry Cyber Partnership.[39]

Before establishing in the Wales Summit that cyber defence is part of NATO's core task of collective defence, the only other cooperation mechanism in regards to cyberspace was NATO's consultation mechanism under Article 4 of the North Atlantic Treaty, which establishes a right to request consultations among Member States.[40] Even though the consultations do not establish grounds to offer physical assistance, they provide for exchange of information, opinions, communications of actions or decision by Member States and discussions with the aim of reaching a consensus on policies to be adopted or actions to be taken. Hence, the consultations could lead to a joint decision or action on behalf of the Alliance.[41]

The Group of Eight (G8) commitment in 2000 to take a concerted approach to high-tech crime such as cybercrime follows from the late 1990s initiatives of forming G8 Subgroup on High-Tech Crime and the network of law enforcement cooperation, fostering speedy communication and formal, real-time assistance in cybercrime investigation. The G8 cooperation in information sharing was expanded to cover protection for critical infrastructure in 2003. The 2009 G8 declaration forwarded the commitment to identifying the solutions needed to strengthen international law enforcement cooperation and to promote forms of partnership between the government and the private sector – including service providers and CERTs. Moreover, it was mentioned that the G8 member states should continue to enhance their cooperation in the sphere of organization of cross-border cybercrime investigations.[42]

In 1992, Organisation for Economic Co-operation and Development (OECD) adopted the Guidelines for the Security of Information Systems to promote international cooperation as well as cooperation between public and private sectors. Similar cooperation promoting guidelines were issued in 1997 for Cryptography Policy, in 2002 for the security of information systems and networks, and in 2008 for the protection of critical information infrastructure. In 2008, the OECD emphasised multi-stakeholder and cross-border cooperation within the Internet economy, and in 2011, the Council Recommendations encouraged multi-stakeholder co-operation in policy development processes as well as promoting Internet security. The Council has continued with the theme in 2012 and 2014 recommendations on the protection of privacy of personal data, and digital government strategies, respectively.[43]

---

[39] *Wales Summit Declaration,* http://www.nato.int/cps/po/natohq/official_texts_112964.htm.
[40] North Atlantic Treaty, Article 4 stating that 'the Parties will consult together whenever, in the opinion of any of them, the territorial integrity, political independence or security of any of the Parties is threatened'.
[41] See NATO The Consultation Process and Article 4. Available at http://www.nato.int/cps/en/natolive/topics_49187.htm (30.10.2014).
[42] G8 summit archive with delegations; declaration and communiqués; other official releases; documents released by national delegations at summits; available transcripts of summit news conferences at University of Toronto: http://www.g8.utoronto.ca/summit/.
[43] OECD forums, ministerial and high-level meetings at http://www.oecd.org/newsroom/oecdforumsministerialandhigh-levelmeetings.htm.

Conclusion

Taking into account *de lege lata* that exists for assistance and cooperation in regards to cyberspace, it can be concluded that the regulation that exists today is mostly scattered around and created by different organisations. Even though there is no single norm that would oblige States to cooperate, many norms, treaty regimes and conventions that States have willingly adopted require cooperation in in different fields and at various occasions.

While there is no exhaustive duty to cooperate, there is no real obstacle to deriving forms of cooperation from or building them on the UN Charter. It is up to the international community and states, in particular, need to decide whether they are willing to reaffirm these provisions in ICT related cooperation. Often enough, the actors take a narrow *lex lata* perspective and conclude that no such norm exists, giving way to the need to ask if new norms are required at all. International law should not be seen as to forbid the international community to develop further detailed arrangements for cooperation on specified goals and issues, such as CERT cooperation and cybercrime prevention, provided there is good will and an identified need. The *lex lata* interpretation, treating international law as only providing responsibility, in fact reduces itself to a mechanism of sanctions that is hardly enforceable between sovereign states. Such an approach cannot satisfy the requirements of the changing world and the arguable need to adopt *de novo* legal instruments.

States do not decide on whether to cooperate or not from an explicitly formulated normative duty, but from the reasons to engage in such activities. They use law, regulations and other instruments to frame, justify, but also to facilitate their decisions and actions. Yet, normative instruments have their own intrinsic value. They are manifestations of cooperation and either directly or indirectly, and often with modest binding force, enhance cooperation. Regardless of its motives and purposes, cooperation can be seen at least as a plausible hypothesis, as a value positively contributing to international peace and security, regional stability and national development and wellbeing.