Science, Technology, and Public Policy Program
Explorations in Cyber International Relations Project

Cyber norm emergence at the United Nations

- An Analysis of the Activities at the UN Regarding Cyber-security

by Tim Maurer

HARVARD Kennedy School
Belfer Center for Science and International Affairs

September 2011

Discussion Paper #2011-11
Explorations in Cyber International Relations Discussion Paper Series

Belfer Center for Science and International Affairs
Harvard Kennedy School
79 JFK Street
Cambridge, MA 02138
Fax: (617) 495-8963
Email: belfer_center@harvard.edu
Website: http://belfercenter.org

Cyber Norm Emergence at the United Nations – An Analysis of the UN's Activities Regarding Cyber-security

By Tim Maurer*

Science, Technology, and Public Policy Program
Explorations in Cyber International Relations Project

Belfer Center for Science and International Affairs
Harvard Kennedy School
79 John F. Kennedy Street
Cambridge, MA 02138
USA

Belfer Center Discussoin Paper 2011-11
September 2011

* The research was undertaken while the author was a fellow at the Global Public Policy Institute in Berlin, Germany (www.gppi.net).

Citation

This paper may be cited as: Maurer, Tim, "Cyber Norm Emergence at the United Nations – An Analysis of the UN's Activities Regarding Cyber-security?", Discussion Paper 2011-11, Cambridge, Mass.: Belfer Center for Science and International Affairs, Harvard Kennedy School, September 2011.

Comments are welcome and may be directed to Tim Maurer, tim.maurer@post.harvard.edu

Funding Acknowledgment

This work is funded by the Office of Naval Research under award number N000140910597. Any opinions, findings, and conclusions or recommendations expressed in this publication are those of the author (s) and do not necessarily reflect the views of the Office of Naval Research.

Abstract

Cyber-warfare is no longer science fiction and the debate among policy-makers on what norms will guide behavior in cyber-space is in full swing. The United Nations (UN) is one of the fora where this debate is taking place and the focus of this paper. The activity at the UN over the course of the past decade exhibits an astonishing rate of norm emergence in cyber-space relative to typical international relations timelines. Most recently, Russia together with China (and Tajikistan and Uzbekistan) proposed an "International code of conduct for information security" in September 2011. In 2010, the U.S. reversed its long-standing policy position by co-sponsoring for the first time a draft resolution on cyber-security that has been introduced in the UN General Assembly by the Russian Federation since 1998. Generally, two principal streams of negotiations regarding cyber-security can be distinguished at the United Nations: a politico-military stream focusing on cyber-warfare and an economic stream focusing on cyber-crime. I highlight the various signs that norms to govern cyberspace are slowly emerging and moving towards norm cascade. At the same time, I show that this process is dynamic. Using the model of a norm life cycle developed by political scientists Martha Finnemore and Kathryn Sikkink my research was therefore guided by the following questions: What exactly have norm entrepreneurs, UN member states and UN organizations, been doing with regard to cyber-security and why was there this variance in activity over time? The first part outlines key definitions and concepts. In part II, I examine the debates among states acting as norm entrepreneurs at the United Nations. This historical analysis is two-fold: I focus on the politico-military stream regarding cyber-warfare first and then on the economic stream on cyber-crime. The third section on the IGF describes the history of this relatively new institution for the sake of comprehensiveness followed by my conclusion.

Table of Contents

Introduction[1]

On January 15, 2011, the New York Times reported, "The biggest single factor in putting time on the [Iranian] nuclear clock appears to be Stuxnet, the most sophisticated cyberweapon ever deployed".[2] Only a few months earlier, Richard D. Clarke, responsible for coordinating cyber-security at the White House until 2003, wrote "Having some effective limits on what nations actually do with their cyber war knowledge might, given our asymmetrical vulnerabilities, be in the U.S. national interest".[3] This tells us three things. First, it reminds us that cyber-warfare is no longer science fiction. Second, the debate among policy-makers in the United States (U.S.) and internationally on what norms shall guide behavior in cyber-space is in full swing. Third, the emerging perception of what constitutes national interest will inform and be informed by the discussions on how to use the new technological possibilities for warfare.

One of the fora where this discussion is taking place is the United Nations (UN), the focus of this paper. Interestingly, while cyber-security was making front page headlines in 2010 with Stuxnet and WikiLeaks, something remarkable took place in a small meeting room at the United Nations: the U.S. reversed its long-time policy position and for the first time co-sponsored a draft resolution on information and telecommunications technology in the context of international security – nowadays usually called 'cyber-security' for short – which has been introduced by the Russian Federation since 1998.[4] In a latest development, the governments of Russia and China (as well as of Tajikistan and Uzbekistan) proposed an "International code of conduct for information security" on September 14, 2011, to be considered at the next session of the UN General Assembly.[5] Moreover, Russia published a concept for a Convention on International Information Security only a week later.[6]

Earlier in 2010 at the UN, a group of governmental experts (GGE) including diplomats from the U.S., Russia, and China, jointly stated "Existing and potential threats in the sphere of information security are among the most serious challenges of the twenty-first century" in its report published in July.[7] A first group established in 2004 failed to even find the smallest common denominator which forced the Secretary-General to conclude in 2005 that "given the

[1] *I would like to thank Joseph S. Nye, Jr. for his helpful comments and support. Special thanks go to the Global Public Policy Institute in Berlin, Germany, particularly to its Associate Director, Thorsten Benner, for hosting me as a Visiting Fellow in the summer of 2010. GPPi's staff provided me with an outstanding stimulating environment and I am especially grateful to Oliver Read for his help in editing the manuscript. Venkatesh "Venky" Narayanamurti at Harvard Kennedy School was crucial for the realization of this paper as well as the patience and support from Michael Sechrist.*

[2] Broad et al, 2011
[3] Clarke and Knake, 2010: 226
[4] UN General Assembly A/RES/53/70
[5] UN General Assembly A/66/359; see Appendix
[6] Russian Federation 2011
[7] UN General Assembly A/65/201: 2

complexity of the issues involved, no consensus was reached on the preparation of a final report".[8]

Two principal streams of negotiations regarding cyber-security can be distinguished at the United Nations: a politico-military stream focusing on cyber-warfare and an economic stream focusing on cyber-crime. Both show signs that norms to govern cyberspace are slowly emerging and moving towards norm cascade. These signs include, for example, the debates in the General Assembly's first committee for more than a decade, the fact that at least half a dozen UN organizations have become involved in the issue most notably in the last five years, and the latest proposals for a code of conduct. This general trend does not explain the variance in the activity however. For example, why was there such a flurry of activity between 1998-2004 followed by the U.S. voting against the Russian draft resolution during the four subsequent years? And what about the negotiations on cyber-crime since the Budapest Convention on Cybercrime entered into force in 2004? My research was therefore guided by the following questions: What exactly have norm entrepreneurs, UN member states and UN organizations, been doing with respect to cyber-security and why was there this variance in activity over time?

It is too early to tell whether the change of position by the U.S. actually constitutes a strategic reversal or if it is more of a tactical move from the Bush to the Obama administration and should be seen in light of the "reset policy" vis-à-vis Russia. Nevertheless, the policy shift together with the GGE's report are political signals important enough to justify a closer look at what is happening at the UN with regard to cyber-security. For example, the Secretary-General of the International Telecommunication Union (ITU) supports a cyber-peace initiative, which is an "attempt to delegitimize cyberwar through reversing the perspective" offering a counter-narrative in a debate that tends to be dominated by terms like cyber-attack, cyber-war[9], or "electronic pearl harbor".[10]

With regard to international relations theory, my findings fit with the norm life cycle model developed by political scientists Martha Finnemore and Kathryn Sikkink. I therefore use their model to guide my analysis. My goal is to shed light on the beginnings of the norm life cycle focusing on the first stage, norm emergence, and the early days of international regimes with regard to cyberspace. As it turns out, the UN has been one of the early and important fora for these debates. What the model does not explain are the ups and downs in the dynamic process of cyber norm emergence.

After the first part on theory outlining key definitions and concepts, I present a historical analysis of the debates on cyber-security among states acting as norm entrepreneurs at the United Nations in part II. The analysis is two-fold focusing, first on the politico-military stream regarding cyber-warfare and then on the economic stream on cyber-crime. I highlight the various phases of this

[8] UN General Assembly A/60/202: 2
[9] See Nye, 2011 3-4 for a brief discussion of the term "cyber-war"
[10] Wegener, 2011: 77; Schwartau 1991

activity and explain how the historic low in U.S.-UN relations in 2005 relates to the downturn from 2005-2008 and how the change in administration was followed by the policy shift from 2008 to 2010 together with first major headlines on the cyber incidents. The subsections on organizational platforms also represent a mapping of the various UN bureaucracies involved in cyber-security. With the latter, I hope to provide the basis for further research examining each platform in greater detail which was beyond the scope of this paper. The third section on the Internet Governance Forum (IGF) describes the history of this relatively new institution for the sake of comprehensiveness followed by my conclusion.

Methodologically, process-tracing is the key technique used for the analysis. Information collected from primary and secondary literature was complemented by interviews with UN officials. I am particularly grateful for their time and support. To protect the interviewees, they are not specifically identified in the text as they have asked to remain anonymous and their identification would be rather easy since most organizations only have a few officials working on cyber-security. However, in most cases their information was substantiated with secondary open source material or, where that was not possible, at least verified by two sources to appear in the text.

I. Theoretical Foundations, Definitions, and Concepts

I.1. Cyber Definitions and International Cooperation*

Cyber as a prefix refers to electronic and computer based technology.[11] Cyber-space is "an operational domain framed by use of electronics to … exploit information via interconnected systems and their associated infrastructure".[12] *Cyber-space* is therefore "a unique hybrid regime of physical and virtual properties", hardware and software, which is all computer networks in the world including the Internet as well as other networks separate from and not linked to the Internet.[13]

The Internet as the biggest network in cyber-space was designed to be "open, minimalist, and neutral".[14] The Internet's architecture however is contingent and "a choice – not fate, not destiny, and not natural law".[15] Alternative manifestations can be found in China or Saudi-Arabia. The "bordered Internet" that emerged through national changes of the Internet's architecture is the result of national laws, technological developments enabling the implementation of certain policies, and on a broader level the preferences of different cultures.[16]

Yet, the Internet remains, from a technological point of view, borderless. Transnational or global would be the corresponding adjectives in international relations theory. While it is true that national legislation does create borders legally and sometimes through specific technical features such as China's Great Firewall, the original design of the Internet ignores national borders. It is designed such that, without governmental interference, it is borderless unless specific interventions are taken to alter this state of nature.

A user can therefore take actions in one country that will have outcomes in another country without the user ever having left their own country. Such action can be benevolent or malevolent while potentially exploiting loopholes in national and international jurisdictions. In case of the latter, the need for international cooperation in handling cyber-security is obvious. As a matter of fact, the Secretary-General of the ITU points out "By some counts, more than six countries have experienced cyber assaults in the past three years and at least 34 private companies were attacked in the early months of 2010 alone".[17]

Cyber-security has been defined by the ITU to mean "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".[18] According to Harvard University professor Joseph Nye, cyber-

[11] For an overview of the International Relations literature and cyber-security, see Eriksson et al; Nazli
[12] Kuehl cited in Nye, 2010: 3
[13] Nye, 2010: 3; Clarke and Knake, 2010: 70
[14] Wu and Goldsmith 2008: 23
[15] Wu and Goldsmith, 2008: 90
[16] Wu and Goldsmith, 2008: 149-150
[17] Toure, 2011: 9
[18] UN ITU-T X.1205 "Overview of Cyber-security": 2

security can be divided into four major threats: espionage, crime, cyber war, and cyber terrorism.[19] The possibility for the existence of a threat in the first place goes back to three sources, "(1) flaws in the design of the Internet; (2) flaws in the hardware and software; and (3) the move to put more and more critical systems online".[20]

Cyber-power "is 'the ability to use cyberspace to create advantages and influence events in 30 other operational environments and across the instruments of power.' Cyber power can be used to produce preferred outcomes *within* cyberspace or it can use cyber instruments to produce preferred outcomes in other domains *outside* cyberspace".[21]

Because of the Internet's transnational nature, governments have recognized the need for international cooperation. Stanford University professor Stephen Krasner famously defined international cooperation in the form of regimes as "sets of implicit or explicit principles, norms, rules, and decision-making procedures around which actors' expectations converge in a given area of international relations".[22] Importantly, while states are the key players in such regimes, they are not the only ones. Other entities such as international organizations also play a role. An international organization can represent a regime or be part of one. The Office of the United Nations High Commissioner of Refugees (UNHCR), for example, stands for the regime centered on the Refugee Convention. At the same time, UNHCR is only a part of the broader humanitarian regime that also includes Unicef, the International Committee of the Red Cross and many others.

Unlike the early principal-agent theories, the work of scholars like Michael Barnett and Martha Finnemore have shown that international organizations have a mind of their own and pursue goals different from what their principals want.[23] This elucidates the point that international organizations must be understood as agents rather than considered simply as structure. Their legitimacy derives from their expertise, delegated and/or moral authority. They induce deference from their principals through the use of their institutional and discursive resources.[24] Moreover, Barnett and Finnemore have shown the power of international organizations and how they exercise their influence in international relations. They highlight that international organizations exercise power in three ways: they "(1) classify the world, creating categories of actors and action; (2) fix meanings in the social world; and (3) articulate and diffuse new norms, principles, and actors around the globe".[25] A very illustrative example is the category of "refugee" that in many countries is directly linked to security matters.[26] In the cyber arena, the ITU Secretary-General together with the World Federation of Scientists propose an alternative frame with the

[19] Nye, 2010: 16
[20] Clarke and Knake, 2010: 73
[21] Nye, 2010: 4 citing Kuehl
[22] Krasner, 1983: 2
[23] Barnett and Coleman, 2005: 597-598
[24] Barnett and Finnemore, 2004: 5
[25] Barnett and Finnemore, 1999: 710
[26] Barnett and Finnemore, 1999: 710-711; Barnett and Finnemore, 2004: 73-120

"cyber peace" agenda in stark contrast to a literature dominated by a terminology including "cyber threat" or "cyber war".

I.2. Norms and the Concept of a Norm Cycle

Stewart Baker, the Department of Homeland Security's first Assistant Secretary for Policy, pointed out on March 4, 2011, at an event titled *Cyber-security: Law, Privacy, and Warfare in a Digital World* that psychological studies suggest that it is part of human nature to feel the need to punish someone who violates a social norm. Political scientists James March and Johan Olsen speak of the logic of appropriateness in addition to the logic expected consequences:

> "Human actors are imagined to follow rules that associate particular identities to particular situations, approaching individual opportunities for action by assessing similarities between current identities and choice dilemmas and more general concepts of self and situations. Action involves evoking an identity or role and matching the obligations of that identity or role to a specific situation. The pursuit of purpose is associated with identities".[27]

In short, norms, including those that structure international affairs, are dynamic and capable of strengthening or weakening over time. The norm of a ban of torture is a recent example of norm erosion. As Baker alluded to, the crucial question is what norms will we chose to guide behaviour in cyberspace.

Finnemore and Sikkink developed their concept of a norm life cycle in their article "International Norm Dynamic and Political Change". Defining "norm as a standard of appropriate behavior for actors with a given identity"[28], they divide the norm life cycle into three stages; the "norm emergence" potentially resulting in a "norm cascade" once the tipping point has been reached which is then followed by the norm's "internalization".[29] Importantly, they point out that a norm cascade or internationalization is not a linear process, nor is the process necessarily completed.

As I describe below, it seems that norms governing cyberspace are still in stage one - norm emergence. This is not surprising given that cyberspace itself is still rather new. Yet, there are already a number of emerging norms in the cyber realm. For instance, both the Clinton and subsequent Bush administrations shied away from authorizing hacking into financial systems to go after terrorists or just before the 2003 Iraq War.[30] In addition, "We have, in effect, what in nuclear war strategy we called a 'withhold target set,' things that we have targeted but do not intend to hit. That policy assumes, or hopes, that opponents will also play by those unarticulated

[27] March and Olsen, 1998: 951
[28] Finnemore and Sikkink, 1998: 891
[29] Finnemore and Sikkink, 1998
[30] Clarke and Knake, 2010: 202

rules".[31] Such provisions are early signs of norm emergence and, if internationally shared, effective limits on the conduct of cyber warfare.

For this first stage, Finnemore and Sikkink point out "The characteristic mechanism of the first stage, norm emergence, is persuasion by norm entrepreneurs. Norm entrepreneurs attempt to convince a critical mass of states (norm leaders) to embrace new norms".[32] Moreover, they identify two elements that have been common to the successful emergence of new norms: (i) norm entrepreneurs, and (ii) organizational platforms that entrepreneurs can use.[33] (Harvard Law School professor Lawrence Lessig uses the terms "meaning architect" in his article "The Regulation of Social Meaning", more or less a synonym to norm entrepreneur.[34] Similarly, John W. Kingdon, professor emeritus at the University of Michigan, uses "policy entrepreneur" but in a broader sense.[35])

I.3. Norm Entrepreneur(s) at the United Nations

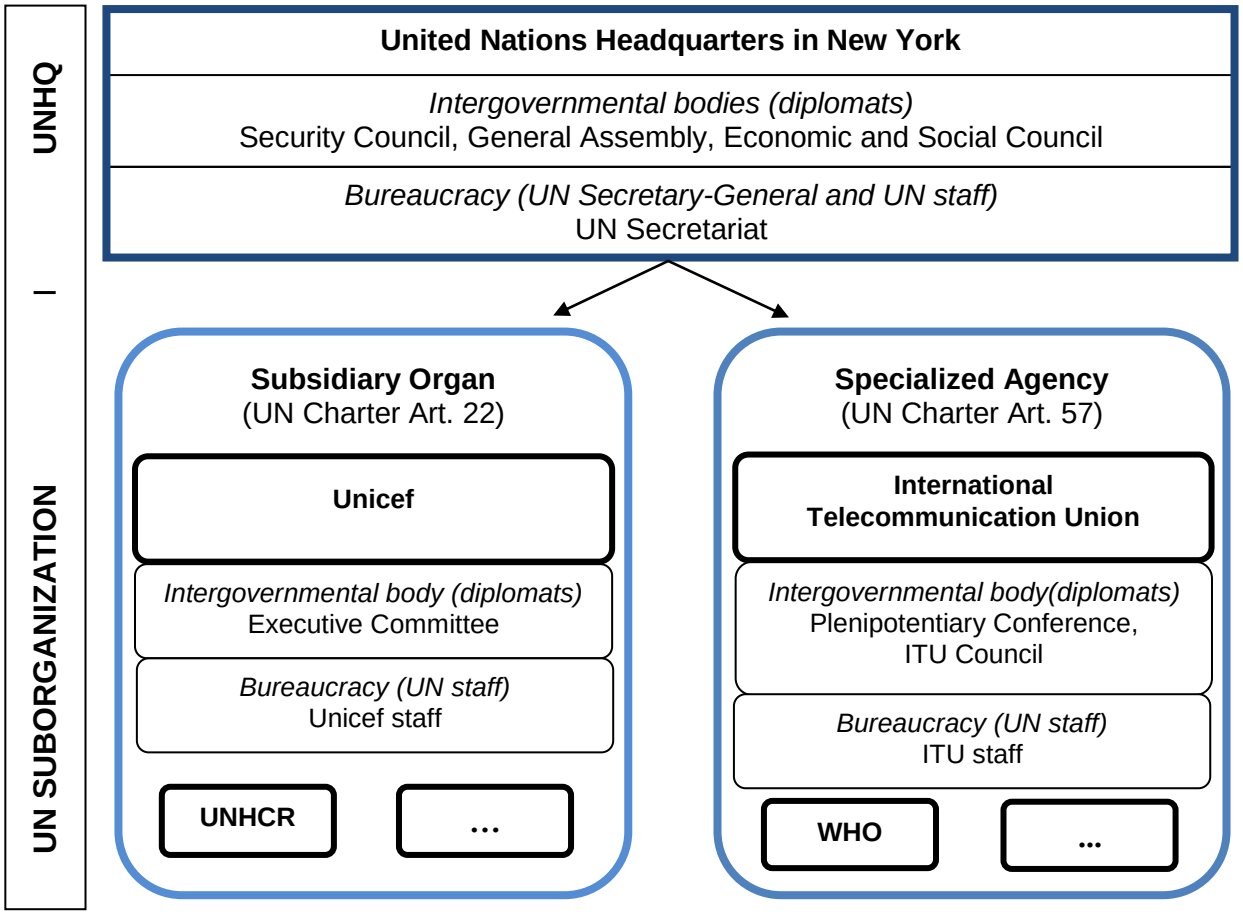
Since David Mitrany's functionalism, often presented in a nutshell as 'form follows function', took hold in international relations theory, academia's understanding of international organizations has advanced tremendously. Generally speaking, an international organization is made up of a plenary intergovernmental body, which takes the decisions, and a bureaucratic apparatus that implements those decisions. The people belonging to the first are diplomats. The people making up the second are staff members or international civil servants. In more recent literature, a group of scholars has shown that the bureaucracies of international organizations operate as autonomous actors under certain conditions. Essentially, the form takes on a life of its own. [36]

Norm entrepreneurs are therefore politicians, diplomats, military service members, academics. Essentially anyone with sufficient resources to exert influence can act as a norm entrepreneur. The UN is important in this context for two reasons. First it is an important forum where such norms and regimes emerge as a result of diplomatic interactions and second, because UN officials are policy entrepreneurs themselves. The role of UN officials as norm entrepreneurs will be elucidated later with a discussion of the cyber-peace initiative supported by ITU's Secretary-General. This fits the remarks by Finnemore and Sikkink describing the UN as an example of a standing organization that can serve as a organizational platform. They highlight that such a platform is often subject to various sometimes competing agendas.[37]

[31] Clarke and Knake, 2010: 203
[32] Finnemore and Sikkink, 1998: 895
[33] Finnemore and Sikkink, 1998: 896
[34] Lessig, 1995
[35] Kingdon, 2003
[36] Barnett and Finnemore, 1999, 2004
[37] Finnemore and Sikkink, 1998: 899

At the heart of the system is the UN Charter. It provides the legal framework which is the most accurate way to conceptualize the relationships between its various entities. Its intergovernmental body consists of three organs: 1) the Security Council with 15 out of the total of 192 member states, 2) the Economic and Social Council (ECOSOC) with 54 members, and 3) the General Assembly with all of the 192 members. Diplomats are the actors in these organs. The bureaucracy to these three organs is what is known as the UN Secretariat headed by the Secretary-General. Its staff is organized in departments. While the diplomats carry diplomatic passports by their governments, UN staff members have separate blue UN passports which illustrate the difference between the intergovernmental body and the bureaucratic apparatus.

This two-level set-up is also present in the design of the UN sub-organizations which are part of the UN system either as a subsidiary organ through article 22 or as a specialized agency under article 57 of the UN Charter. The legal architecture of the UN system has a clear hierarchy built into it. A visualization is shown below bearing in mind that the structure of an individual organization might differ from this generalization. This legal hierarchy is why my analysis focuses on and is limited to the core of the UN Charter e.g., the intergovernmental bodies of the Security Council, ECOSOC and the General Assembly. The dynamics in other intergovernmental bodies are beyond the scope of this paper and points for future research. This includes ITU's governing body, the United Nations Congress on Crime, or the Conference of the parties to the UN Convention against Transnational Organized Crime. The intergovernmental bodies of UNODC are included in this paper because they are functional commissions of ECOSOC. For the purposes of this analysis, I treat the others as organizational platforms as described by Finnemore and Sikkink with the exception of the ITU, which plays a dual role as highlighted below.



I.4. Norms and International Law

The Security Council is the only legitimized authority to create binding international law according to Article 25 of the UN Charter that states "The Members of the United Nations agree to accept and carry out the decisions of the Security Council in accordance with the present Charter". The UN General Assembly on the other hand can only make recommendations according to Article 10 and 12 of the UN Charter. It is important nevertheless. Why?

Since legal scholar Lord McNair's *The Functions and Differing Legal Character of Treaties* published in 1930, a number of scholars have discussed the difference between soft and hard law in international law. Soft law is in written form but not a source of law in the sense of Article 38 (1) (a) of the ICJ Statute.[38] According to law professor Alan E. Boyle it differs from hard law in three ways since it is not binding, not readily enforceable through binding dispute resolution, and consists of general norms or principles while at the same time it is designed to influence state practice.[39] Kenneth W. Abbott, law professor at Arizona State University, and Duncan J. Snidal, political science professor at the University of Chicago, label these dimensions of soft law as

[38] Chinkin, 1989; Hillgenberg, 1999
[39] Boyle, 1999

differences in obligation, precision, and delegation.[40] The resolutions of the General Assembly discussed below fall into this category of soft law. Resolutions of ECOSOC, however, have less weight since ECOCOC's limited membership does not have as much legitimacy as the General Assembly representing all member states of the UN.

The activity in the General Assembly therefore matches what we would expect from the literature on soft law, which outlines that soft law is sometimes preferred over hard law because of "the need to stimulate developments still in progress" and "the creation of a preliminary, flexible regime possibly providing for its development in stages" since "it has frequently been the case that a text which has been laid down at a conference as a non-treaty-binding standard [Hillgenberg uses this term as a synonym for soft law[41]] gradually becomes, as awareness grows, a binding and possibly a 'hard' obligation".[42]

In sum, the literature on soft and hard law shows that soft law plays an important role in international relations. It can lead to an international treaty or exist in addition to a treaty. Finnemore and Sikkink point out in their work that "Understanding which norms will become law ('soft law' as well as 'hard law') and how, exactly, compliance with those laws comes about would seem, again, to be a crucial topic of inquiry that lies at the nexus of law and IR" because these legal rules guide and determine the political actors' behavior.[43] The following pages hopefully help understand this process with regard to norms governing cyberspace.

[40] Abbott and Snidal, 2000
[41] Hillgenberg, 1999: 500
[42] Hillgenberg, 1999: 501; see also Boyle, 1999: 904; Chinkin 1989: 856, Abbott, and Snidal, 2000: 447. For a more detailed account on the State's reasons for choosing soft over hard law arrangements see Abbott and Snidal, 2000.
[43] Finnemore and Sikkink, 1998: 916

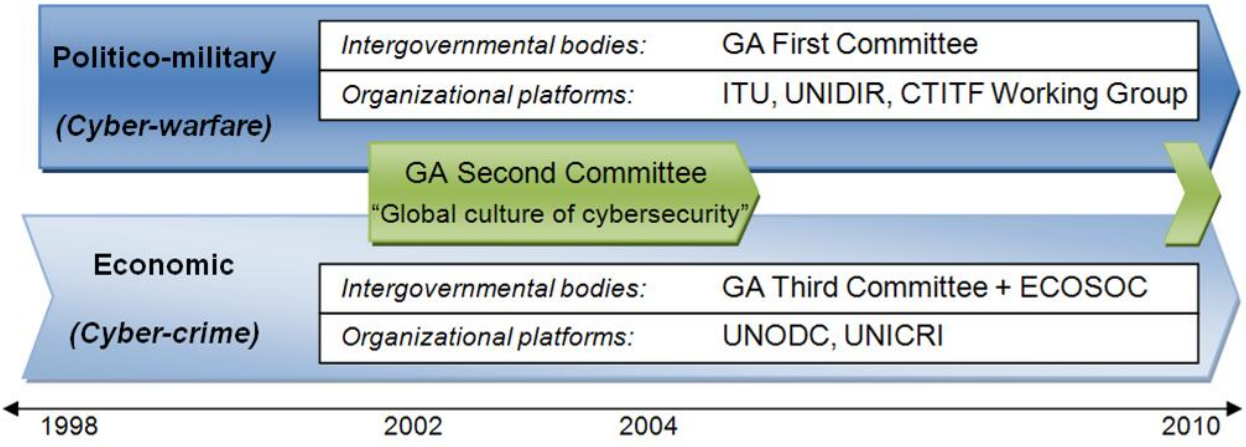
II. Cyber-security and the United Nations

The norm emergence process at the United Nations regarding cyber-security can be divided into two main streams of negotiations: negotiations focusing on what I will call in short "politico-military" issues and a second stream of negotiations on "economic" issues. The politico-military stream is in UN language concerned about how "[information] technologies and means can potentially be used for purposes that are inconsistent with the objectives of maintaining international stability and security and may adversely affect the security of States".[44] The economic stream in turn is about "the criminal misuse of information technologies".[45]

Cyber-warfare and cyber-crime are alternative terms for the two streams, respectively. Clarke and Knake define cyber-warfare as "the unauthorized penetration by, on behalf of, or in support of, a government into another nation's computer or network, or any other activity affecting a computer system, in which the purpose is to add, alter, or falsify data, or cause the disruption of or damage to a computer, or network device, or the objects a computer system controls".[46] Nye mentions some additional points that relate to defining the term in a broader, non-legalistic sense.[47]

There are a number of arguments against using any of the four terms but for the purpose of this paper, an in-depth discussion is beyond the scope of my analysis. I would like to point out, however, that in addition to these questions of framing there is a set of questions about whether "warfare" or "crime" are adequate terms to describe certain actions in cyber-space in the first place. This set of questions is particularly important in light of the missing dimension of territory in cyber-space which is so important for traditional legal definitions of war and battlefield.

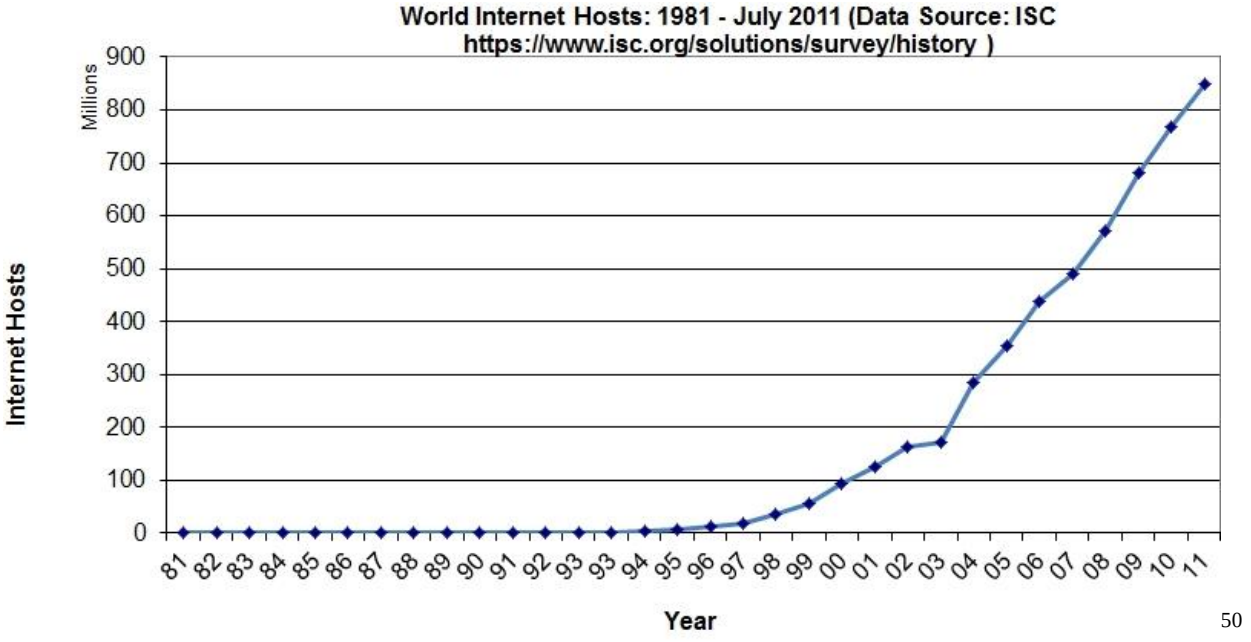
Cyber-security Norm Emergence Process at the United Nations: Two Streams Model



[44] UN General Assembly A/RES/53/70
[45] UN General Assembly A/RES/55/63
[46] Clarke and Knake, 2010: 227
[47] Nye, 2011

One could add a third stream centering on the IGF, which addresses broader Internet governance questions relating to the role of the Internet Corporation for Assigned Names and Numbers among others. However, these negotiations have not been directly dealing with cyber-security and the IGF has only been around for five years. That is why they are briefly discussed in part III to present a comprehensive picture but not treated as a separate analytical unit and stream. Also, the ITU lists Unicef as a partner of the Child Online Protection initiative. Unicef's activities on cyber-security however are generally very limited.[48]

A brief explanation on why the timeline starts with the year 1998. There are two reasons. First, 1998 was the first year that the Russian government introduced a resolution in the First Committee. There are resolutions referencing computer-related crimes that were adopted prior to 1998 such as General Assembly resolution 55/63 mentioning the Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders in 1990. However, I focus on the First Committee because 1998 coincides with another important development, the exponential growth of the Internet that starts in the late 1990s as shown below. (That is also why the year 1995 is often considered to be "year zero".[49]) This growth is correlated with the exponential growth in the number of Internet users which created greater interdependence and an increased threat level.



50

[48] Unicef; UN ITU "Child Online Protection"
[49] Carr, 2010
[50] Wikipedia "The History of the Internet"

The negotiations among member states in the UN's intergovernmental bodies regarding cyber-security can be summed up with the excerpt from an interview between the Bulleting of the Atomic Scientists and Ronald Deibert, professor of political science and director of the University of Toronto's Citizen Lab:

> "*Bulletin of the Atomic Scientists*: The United States has been pushing for broader cooperation on the crime-fighting level, and Russia has been calling for "cyber arms control." Is this achievable?
>
> *Deibert*: Russia has been pushing for arms control in cyberspace, or information-weapons control. Most people dismiss this as disingenuous, and I tend to agree. Most observers see it as Russia's attempt to constrain U.S. superiority in the cyber domain. Russia is more concerned about color revolutions and mobilization on the Internet by dissident and human rights groups – and trying to eliminate the United States' ability to support that type of social mobilization – than it is about protecting the Internet. In spite of that, I think it's worthwhile to push them on it. If I were working for a foreign affairs ministry, I'd use this as an opening to talk about mutual restraint, cooperation, and push them back on what should be the rules of cyberspace".[51]

Or, as The New York Times puts it:

> "The Russians have focused on three related issues, according to American officials […] In addition to continuing efforts to ban offensive cyberweapons, they have insisted on what they describe as an issue of sovereignty calling for a ban on 'cyberterrorism.' American officials view the issue differently and describe this as a Russian effort to restrict 'politically destabilizing speech.' The Russians have also rejected a portion of the Council of Europe Convention on Cybercrime that they assert violates their Constitution by permitting foreign law enforcement agencies to conduct Internet searches inside Russian borders."[52]

In his June 2010 article, Wall Street Journal reporter Siobhan Gorman also points out that the U.S. considers a treaty premature based on the concern that a treaty would not prohibit countries like Russia and China to use third parties to circumvent the treaty.[53]

The Security Council's involvement has been largely limited to the work of the Working Group on Countering the Use of the Internet for Terrorist Purposes which is part of the Counter-Terrorism Implementation Task Force (CTITF). The Council's resolutions do not mention the cyber aspect, for example, in its resolution on Georgia in 2008. (There were no resolutions on Estonia in 2007 or Iran in 2010.)

ECOSOC opened its 2010 session with a briefing titled "Cyber security: emerging threats and challenges".[54] Two of its functional commissions the Commission on Narcotic Drugs and the

[51] Deibert, 2011: 6
[52] Markoff and Kramer, 2009
[53] Gorman, 2010

Commission on Crime Prevention and Criminal Justice have also been dealing with the criminal use of cyber-space.

The General Assembly has seen a lot of activity and discussion on norms governing the behavior of member states, for example, the elements attached to two of its resolutions (see appendix). Three out of the General Assembly's six committees have met to negotiate draft resolutions pertaining to cyber-security. Like all draft resolutions, they were then submitted to the plenary for adoption at the General Assembly's annual session in the fall. These draft resolutions were submitted by the following committees:

> *First Committee (Disarmament and International Security Committee)*, concerned with disarmament and related international security questions; the
>
> *Second Committee (Economic and Financial Committee)* concerned with economic questions; and the
>
> *Third Committee (Social, Humanitarian and Cultural Committee)* deals with social and humanitarian issues.

There have been a total of five groups of governmental experts on cyber related issues so far. The first GGE in 2004 created by the General Assembly's First Committee with the second one publishing its report in 2010. In 2004, ECOSOC set up an intergovernmental expert group on identity-related crime which has evolved into the core group of experts. The ITU set up a high level expert group that developed the cybersecurity agenda in 2007 and the United Nations Congress on Crime Prevention and Criminal Justice established an open-ended intergovernmental expert group on cybercrime in 2010.

Throughout their negotiations, member states have been using UN organizations as organizational platforms for their competing agendas. That is also why the UN's activities regarding cyber-security are highly fragmented. As shown in my subsequent analysis, there is some interesting expertise scattered throughout the system. The ITU divides the UN organizations' work on cyber-security as follows:

> (1) Combating cybercrime: ITU and UNODC;
>
> (2) Building capacity: ITU, UNIDIR, and UNICRI;
>
> (3) Child Online Protection: ITU, Unicef, UNICRI, UNODC.[55]

However, this division is incomplete. It is, for example, not clear why the Child Online Protection initiative and UNODC's training of law enforcement officials are not also a form of capacity-building or why the United Nations Interregional Crime and Justice Research Institute

[54] Toure, 2011: 92; ECOSOC "2010 ECOSOC General segment briefing"
[55] UN ITU, March 2010: 36

(UNICRI) is not mentioned in combating cybercrime. Part II of my paper aims to present a comprehensive picture.

Generally, the ITU and UNODC are considered the lead UN bodies in cyber-security and cyber-crime.[56] That is why the ITU Secretary General and UNODC Executive Director decided to establish formal collaboration among their organizations. In addition, the UN Secretariat in New York assisted the aforementioned CTITF Working Group through its Department of Political Affairs as well as the Institute of Disarmament Research (UNIDIR). UNICRI has focused on cyber-crime.

Analyzing the work of these organizations is important not only from an organizational platform point of view but also because UN bureaucrats themselves can act as norm entrepreneurs in addition to member states. Finnemore and Sikkink remind us that, "Norms do not appear out of thin air; they are actively built by agents having strong notions about appropriate or desirable behaviour in their community".[57] These agents have influence because of their agenda-setting power and their power to "frame" or " 'create' issues by using language that names, interprets, and dramatizes".[58] As Barnett and Finnemore highlight, autonomously acting bureaucracies of international organizations are among these norm entrepreneurs. That is why they are active members in a regime and active members in creating a regime. The ITU, as described below, is a good example of a UN bureaucracy acting independently as a norm entrepreneur.

The next sections present an analysis of the aforementioned streams. As shown in the figure above, the analysis of each stream is divided into two subsections. First, I focus on member states and their negotiations in the intergovernmental bodies. The second subsection examines how the bureaucracies of UN organizations are used as organizational platforms by member states.

[56] UN ITU "PowerPoint Presentation"
[57] Finnemore and Sikkink, 1998: 896
[58] Finnemore and Sikkink, 1998: 897

II.1. The Politico-Military Stream: Cyber-warfare

Clarke writes in his book, "The United States, almost single-handedly, is blocking arms control in cyberspace. Russia, somewhat ironically, is the leading advocate […] since the Clinton administration first rejected the Russian proposal, the U.S. has been a consistent opponent of cyber arms control. Or, to be completely frank, perhaps I should admit that I rejected the Russian proposal […]it may be time for the United States to review its position on cyber arms control and ask whether there is anything beneficial that could be achieved through an international agreement".[59]

This debate is at the center of negotiations in the General Assembly's First Committee on "Developments in the field of information and telecommunications in the context of security" which is the first part of this section. The second part examines how notably UNIDIR and the ITU have been used in this context as organizational platforms.

II.1.1. The First Committee of the General Assembly

The Russian government first introduced a draft resolution on "Developments in the field of information and telecommunications in the context of security" in the First Committee in 1998 and every year since then. It is based on a letter sent by the Russian Minister of Foreign Affairs at the time, Igor Ivanov, to the UN Secretary-General on September 23, 1998, requesting circulation of such a draft resolution.[60] Sergey Ivanov, Minister of Defense from 2001 to 2007, later stated that "Russia wants to develop 'international law regimes for preventing the use of information technologies for purposes incompatible with missions of ensuring international stability and security".[61]

The interaction in the General Assembly has been dominated by the interaction between Russia and the U.S. as alluded to by Clarke. This can be seen by the introduction and sponsorships of draft resolutions as well as voting patterns. Russia is calling for a cyber arms control treaty, whereas the U.S. policy has evolved into the position expressed by one diplomat that "The same laws that apply to the use of kinetic weapons should apply to state behavior in cyberspace" while trying to step up international cooperation among law enforcement agencies.[62] Given the particular attention China has attracted in the media over the last two years with regard to cyber-security, China's relative quiet on the issue at the General Assembly is noteworthy.

[59] Clarke and Knake, 2010: 218-219
[60] Streltsov, 2007
[61] Ford, 2010: 65
[62] Ford, 2010: 67; Markoff, 2010

Phase 1: 1998-2004 – First Steps Towards Cyber Norms. The 1998 draft resolution was adopted as Resolution 53/70 on 4 January 1999. It built on the previous work on the "Role of science and technology in the context of security, disarmament and other related fields" (A/53/576, 18 Nov 1998). The key elements of the resolution for *an* "international computer security treaty"[63] are:

- mentions the military potential of information and communication technology for the first time[64] as well as an expression of concern about the use of such technology "inconsistent with the objectives of maintain international stability and security"[65] (Russian position)
- mentions need to prevent cyber-crime and cyber-terrorism (US position)
- invites member states to inform the Secretary-General notably on their views regarding "definitions" and the development of "international principles" (operative paragraphs regarding next steps).

The two key changes from this first draft of the resolution compared with its 2010 version, which marked the first time that the U.S. co-sponsored the draft resolution after having voted against it between 2005-2008, are:

- Omission of the reference and attempt to come up with definitions which would have arguably been a first step towards a cyber arms control treaty
- Substitution of the reference to "international principles" with references to "international concepts" and "possible measures".

The first resolution on this item, 53/70, was adopted by the General Assembly without a vote. Yet, the push for an international treaty was met with skepticism by the U.S. and European states suspicious that such a treaty could be used to limit the freedom of information under the guise of increasing information and telecommunications security. Christopher A. Ford, senior fellow at the Hudson Institute, concludes his analysis on Russian cyber policy stating "Russian approaches to information warfare and its cyberspace applications have placed considerable emphasis on controlling the content of mass media, with an eye toward shaping both foreign and domestic perceptions".[66] He cites the Russian government's attempts at direct censorship in the 1990s and also the 2000 Information Security Doctrine.[67]

At the same time, the U.S. had an incentive not to limit the use of such technology given that it was and still is considered to be the leader in this field according to Sergei Komov, Sergei Korotkov and Igor Dylevski, experts at the Ministry of Defense of the Russian Federation. They highlighted this point in their 2007 article "Military aspects of ensuring international information security in the context of elaborating universally acknowledged principles of international law"

[63] Markoff, 2010; for literature on a cyber arms convention see for example Geers, 2010; Ford, 2010.
[64] Streltsov, 2007
[65] UN General Assembly A/RES/53/70
[66] Ford, 2010: 59
[67] Ford, 2010: 60+61

that appeared in an issue of Disarmament Forum, a publication by UNIDIR.[68] Ford points out that "The common belief that Russia fears a cyber arms race with the United States is accurate. Some Russian officials have said as much".[69] This also seems to be the perception among Chinese officials as recorded in Clarke and Knake's book with reference to the Revolution in Military Affairs and the role of information technologies during the 1990/91 Gulf War.[70]

Phase 2: 2005-2008 – Stepping Backward, Signs of a Dynamic Process. In 2005, an important change took place in the First Committee. The draft resolution introduced by Russia is adopted but goes to a recorded vote for the first time in its history. The U.S. is the only country voting against the resolution on October 28.[71] It is President George W. Bush's second term and a historic low in UN-U.S. relations after the failed 2005 World Summit. After the U.S. voted against the resolution in 2005, the draft resolution in 2006 (A/C.1/61/L.35) is no longer sponsored by the Russian Federation alone. Instead, the People's Republic of China as well as Armenia, Belarus, Kazakhstan, Kyrgyzstan, Myanmar, Tajikistan, and Uzbekistan co-sponsor the draft and are joined by others in subsequent years.[72] Interestingly, the American opposition set the stage for a multilateralization of the resolution's sponsorship as shown in the graphic on sponsorship below, arguably elevating the issue among member states.

The first GGE established in 2004 was due to present a report in 2005 but ultimately failed to come to a common position forcing the Secretary-General to conclude that "given the complexity of the issues involved, no consensus was reached on the preparation of a final report". This outcome is rather unusual at the UN where an activity is usually only initiated when it is clear before it starts that there is at least some smallest denominator that everyone can agree on so everyone can save face even if the endeavor fails. The Group consisted of governmental experts from 15 States: Belarus, Brazil, China, France, Germany, India, Jordan, Malaysia, Mali, Mexico, the Republic of Korea, the Russian Federation, South Africa, the United Kingdom of Great Britain and Northern Ireland, and the United States of America. They met three times and unanimously elected Andrey V. Krutskikh of the Russian Federation as its Chairman.

According to A.A. Streltsov, a member of the Russian delegation at the GGE meetings and member of the Cryptography Academy of the Russian Federation, "The main stumbling block was the question of whether international humanitarian law and international law sufficiently regulate the security aspects of international relations in cases of 'hostile' use of ICTs for politicomilitary purposes. However, the work of the GGE was not in vain. It successfully raised the profile of the relevant issues on the international agenda."[73]

[68] Komov et al, 2007
[69] Ford, 2010: 62
[70] Deibert, 2011: 3
[71] UN General Assembly A/60/452
[72] UN General Assembly A/C.1/61/L.35; UN General Assembly A/61/389
[73] Streltsov, 2007: 6+7

During the same period, cyber-warfare makes major headlines for the first time in 2007 with the Distributed Denial of Server (DDoS) attack against Estonia and in 2008 during the Georgian-Russian war. (With the caveat that even the description of these two events as "cyber-warfare" is dependent on the still ongoing norm emergence and the emerging consensus on how to classify such incidents. At present, for example, it is still controversial whether DDoS is a cyber-attack or a form of protest to be protected under First Amendment provisions.[74] Intent is one dimension of this ongoing debate. The effects of Stuxnet on the other hand seem more like sabotage than a traditional attack.[75] This suggests that outcome is another crucial factor if a similar type of technique would be used not to sabotage industrial facilities but cause direct physical harm. In short, the debates are as much about norms as on how to classify the world in the first place.)

Phase 3: 2009-2011 – Forward Again. Starting in October 2009, draft resolutions in the First Committee are again adopted without a vote as during the pre-2005 period. The Bush administration has been succeeded by the administration of President Obama who pursues not only a "reset" policy with regard to Russia but also in the United Nations. In fact, the New York Times reported that in November 2009,

> "a delegation led by Gen. Vladislav P. Sherstyuk, a deputy secretary of the Russian Security Council and the former leader of the Russian equivalent of the National Security Agency, met in Washington with representatives from the National Security Council and the Departments of State, Defense and Homeland Security. Officials familiar with these talks said the two sides made progress in bridging divisions that had long separated the countries. Indeed, two weeks later in Geneva, the United States agreed to discuss cyberwarfare and cyber-security with representatives of the United Nations committee on disarmament and international security".[76]

Moreover, in January 2010, the Obama administration presented a position paper with the objective to bring the various parties closer together.[77] Later in the year, the second GGE eventually presented its report. This time the GGE did come to a consensus stating that "Existing and potential threats in the sphere of information security are among the most serious challenges of the twenty-first century". They identify criminals, terrorists, and states as potential perpetrators. Individuals, businesses, national infrastructures, and governments are identified as potential victims. The threat is considered to be large enough to pose a risk to "international peace and national security" as states are found to develop cyber warfare capabilities. They acknowledge the attribution problem and the "dual-use" character of the cyber-space, which corresponds with the idea that the Internet is neutral and the way it is put to use dependent on the intent of its users (unanticipated consequences aside). It mentions existing efforts to combat the

[74] I thank Oliver Read for this thought.
[75] I thank Joseph Nye for this thought.
[76] Markoff and Kramer, 2009
[77] Markoff, 2010

criminal use of information technology and to create a "global culture of cyber security". The group makes the following five recommendations "for the development of confidence-building and other measures to reduce the risk of misperception resulting from ICT disruptions":

1. Further dialogue among States to discuss norms pertaining to State use of ICTs, to reduce collective risk and protect critical national and international infrastructures;
2. Confidence-building, stability, and risk reduction measures to address the implications of State use of ICTs, including exchanges of national views on the use of ICTs in conflict;
3. Information exchanges on national legislation, national ICT security strategies and technologies, policies and best practices;
4. Identification of measures to support capacity-building in less developed countries; and
5. Finding possibilities to elaborate common terms and definitions relevant to United Nations General Assembly resolution 64/25"[78]

The representatives from the U.S. and Russia, Ms. Michele G. Markoff and Mr. Andrez V. Krutshikh, are the only experts from the first GGE who were also part of the second GGE with the latter being elected as chairman of both groups. Markoff first served in her capacity as Senior Coordinator for International Critical Infrastructure Protection at the Bureau of Political Military Affairs and then as Senior Policy Adviser at the Office of Cyber Affairs at the State Department. Krutshikh was the Deputy Director of the Department for Disarmament and Security Matters, before moving to the Department of New Challenges and Threats at the Ministry of Foreign Affairs of the Russian Federation. Interestingly, Estonia and Israel joined the new group established in 2009. Estonia having been the first country to suffer a massive DDoS attack, and Israel being considered as one of the potential states designing Stuxnet.[79]

During this same period when the major WikiLeaks releases and Stuxnet are taking place, the U.S., for the first time, decides to co-sponsor the Russian draft resolution in the First Committee. This echoes Clarke's latest thinking on the topic outlined in his book, "Perhaps I should admit that I rejected the Russian proposal […] the U.S. had to stand almost alone in the UN in rejecting cyber talks, we said no […] and we have kept saying no for over a decade now […] it may be time for the United States to review its position on cyber arms control".[80] Resolution 65/41 also includes a new paragraph requesting the Secretary-General to establish a new GGE in 2012 to submit a report at the 68th session in 2013. Unlike during the first phase however, the resolution is now not only sponsored by Russia but also co-sponsored by three dozen countries including the People's Republic of China.[81]

[78] UN General Assembly A/65/201
[79] Broad et al, 2011
[80] Clarke and Knake, 2010: 218-219
[81] UN General Assembly A/65/405

The media reported on these events as follows. The Washington Post wrote in its article titled "15 nations agree to start working together to reduce cyberwarfare threat" that "A group of nations -- including the United States, China and Russia -- have for the first time signaled a willingness to engage in reducing the threat of attacks on each others' computer networks". Pointing out that "The Russians proposed a treaty in 1998 that would have banned the use of cyberspace for military purposes", the journalist quotes Robert Knake as considering the new development as being "part of the Obama administration's strategy of diplomatic engagement" because in the words of an Obama administration official "There's been an increased understanding of the international need to address the risk".[82]

Nye offers the following assessment of the new environment,

> "For more than a decade, Russia has sought a treaty for broader international oversight of the Internet, banning deception or the embedding of malicious code or circuitry that could be activated in the event of war. But Americans have argued that measures banning offense can damage defense against current attacks, and would be impossible to verify or enforce. Moreover, the United States has resisted agreements that could legitimize authoritarian governments' censorship of the internet. Nonetheless, the United States has begun formal discussions with Russia. Even advocates for an international law for information operations are skeptical of a multilateral treaty akin to the Geneva Conventions that could contain precise and detailed rules given future technological volatility, but they argue that like minded states could announce self governing rules that could form norms for the future".[83]

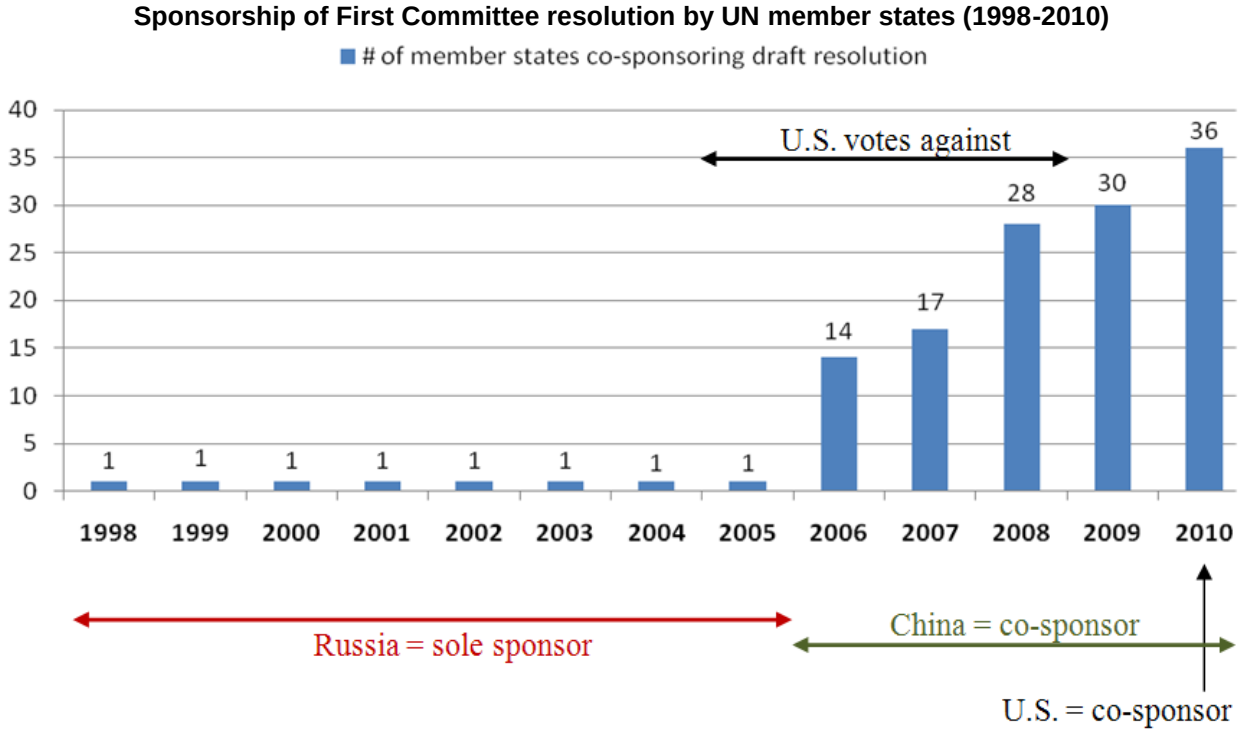
The most recent development is a joint letter issued by the governments of Russia, China, Tajikistan, and Uzbekistan and sent to the UN Secretary-General. Within the letter was included a draft "International code of conduct for information security" (see appendix).

In a first analysis, Adam Segal of the Council on Foreign Relations highlights the following points that are likely to be controversial.[84] First, those who subscribe to the code "endeavour […] to prevent other States from using their resources, critical infrastructures, core technologies and other advantages to undermine the right of the countries, which accepted this Code of Conduct, to independent control of information and communications technologies or to threaten the political, economic and social security of other countries". This seems to contradict the idea of Internet freedom while it represents the traditional international relations principle of non-interference that is the basis for so many disagreements. Second, the code of conduct puts states and multilateral cooperation at the center. However, Internet governance has traditionally not been dominated by states but rather the private sector and civil society. This is the "multilateral" (states only) vs. "multi-stakeholder" (states plus private sector and civil society) debate. (See

[82] Nakashima, 2010
[83] Nye, 2010: 18
[84] Segal, 2011

also Alexey Sidorenko's comments at http://censorshipinamerica.com/2011/09/24/russia-cyber-security-code-of-conduct/).

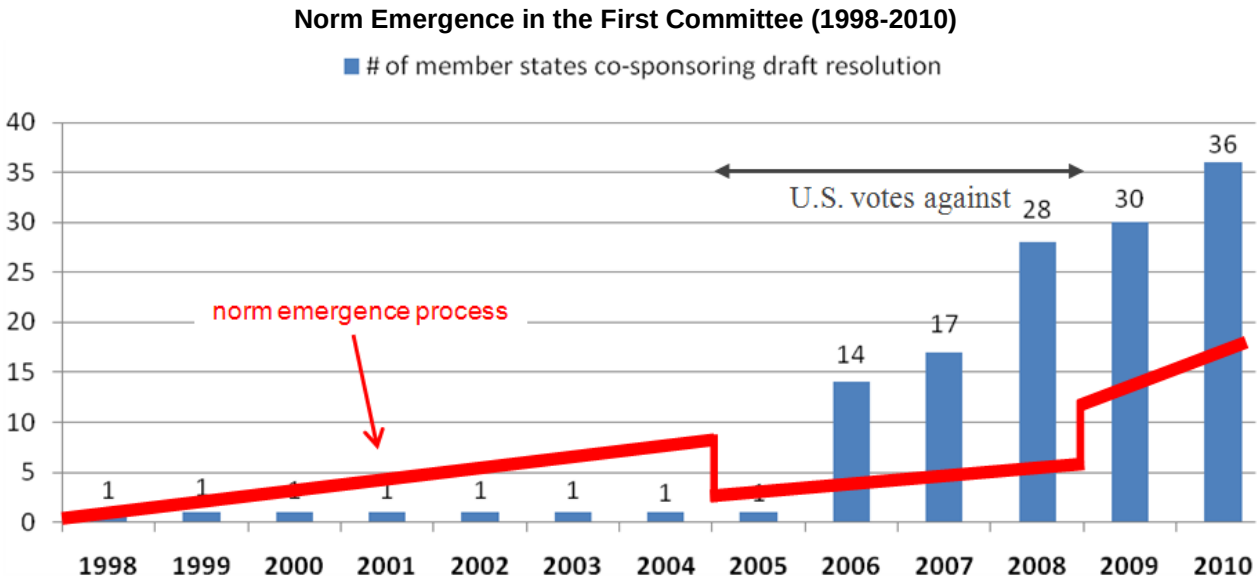
Looking back, the following picture emerges based on the analysis of the activity in the First Committee substantiating the conclusion that negotiations are in the early stages of norm emergence,



My paper does not attempt to develop universal variables to measure norm emergence. For the purpose of this research, the empirical basis for my conclusion that norm emergence is taking place at the United Nations with regard to cyber-security can be found in quantitative and qualitative variables. An example of the former is the number of co-sponsors of a draft resolution indicating an increased interest and support for a resolution within the international community. Another quantitative measure is voting patterns; if a resolution is adopted without a vote, a recorded vote, or even has some member states voting against it, it illustrates the importance and positions member states take toward a specific resolution.

I use these two variables as an example to visualize what I interpret as norm emergence in the First Committee. The sections below further detail this norm emergence process, however, the multiplicity of actors, types of actions, and timeline diminishes the usefulness of a graphic display. The graphic below hopefully provides a basic understanding of how the norm emergence process looks in the First Committee. It highlights the dynamic nature of norm emerges, as shown during the period from 2005-2008 where two opposite trends took place

simultaneously. First the norm slowly emerges after the first draft resolution is introduced by Russia in 1998. The slope of the trend line is >0 because it steadily attracted enough attention to be introduced every year, but remained singularly sponsored by Russia through 2005. In 2005, the U.S. decides to vote against the resolution, thus disrupting the quiet momentum of the norm emergence. This is visualized through a sharp drop in the norm emergence trend line that year. This four-year period of American opposition, however, also sees the number of co-sponsors rise, which is why the slope during this time is >0 and increases after 2009 when the U.S. decides to allow an adoption without vote again.



This is obviously only a very basic model to measure and visualize the norm emergence process. There are also many qualitative variables to consider such as the type of activity, e.g. the actual content of a resolution, the language used in resolutions – takes note, welcomes, invites, requests, etc – whether certain principles are agreed upon and potentially added to a resolution in form of an annex, whether a group of governmental experts is created and whether the group actually produces a report. Another variable is the number of organizational entities dealing with issue and the quantity of activity overall, e.g. number of resolutions, number of projects and program by organization). These are the variables that guide what I present in this paper.

II.1.2. Organizational Platforms: ITU, UNIDIR, and the CTITF Working Group

The United Nations Institute for Disarmament Research

UNIDIR in Geneva was one of the first UN bureaucracies to become involved in cyber-security. At present, Germany funds ongoing research titled "Perspectives on Cyber War: Legal Frameworks and Transparency and Confidence Building" with the objective of raising awareness of the issue among diplomats and sparking further multilateral discussions. UNIDIR's partner is Hamburg University's Institute for Peace Research and Security Policy.[85] In addition, two UNIDIR staff members, J. Lewis and Kerstin Vignard, served the GGE 2010 as consultants from November 2009 to July 2010.[86] Importantly, UNIDIR hosted two conferences relating to the discussions in the General Assembly's First Committee:

In 1999, a year after Russia introduced the first draft resolution in the First Committee, the United Nations Department for Disarmament Affairs funded a two-day discussion meeting from August 25–26 on "Developments in the field of information and telecommunication in the context of international security", the same title as the resolution on this topic.[87] Over seventy participants from more than forty countries attended the event.[88] The discussion summary reveals that the threat assessment and recognition of general problems such as the attribution problems were already known in 1999.

At the same time, states had different primary concerns. Some states cite cyber-crime and cyber-terrorism as the primary issue. Others are more concerned about cyber-warfare. It was also discussed whether discussions should be limited to the Internet or its underlying physical infrastructures. The discussion summary highlights one approach to defining the problem distinguishing three categories: (i) Revolution in Military Affairs dimension, ii) information propaganda focused on persuasion, (ii) critical infrastructure protection and information assurance.[89] This seems to match and emulate the division into "information-psychological" and "information-technical" that Ford considers characteristic of Russia's approach to cyber-security.[90]

In 2008, Russia funded a second such event from April 24-25 titled "Information & Communication Technologies and International Security" with the objective "To examine the existing and potential threats originating from the hostile use of information and communication technologies, discuss the unique challenges posed by ICTs to international security and possible responses".[91]

[85] UNIDIR "Research Project – Perspectives on Cyber War"
[86] UNIDIR "Research Project – GGE"
[87] UNIDIR "Conference – Developments"
[88] UNIDIR *Summary*
[89] UNIDIR "Conference – Developments"
[90] Ford, 2010: 57
[91] UNIDIR "Conference - ICT and international security"; UNIDIR *Agenda*

In addition to these activities, UNIDIR devoted the third issue of its publication Disarmament Forum in 2007 to the issue of Information & Communication Technologies and International Security.[92] The articles in the issue focus on Internet governance, cyber-terrorism, critical information infrastructure, legal issues, and military aspects. The first is written by Henning Wegener, the retired German ambassador and Chairman of the World Federation of Scientists' Permanent Monitoring Panel on Information Security, who wrote the chapter on cyber-peace in the organization's aforementioned publication. In addition, two scholars contribute to the issue as well as four officials from the Russian government.

The International Telecommunication Union

"The International Telecommunication Union (ITU) is the United Nations organization that has most responsibility for practical aspects of cyber-security".[93] It is a treaty organization; in fact, it is the only UN organization working on cyber issues with the status of treaty organization. It is located in Geneva and existed prior to the UN's founding. It subsequently joined the UN system as a Specialized Agency under article 57 of the UN Charter. It plays an important role in setting technical standards and is run by a large technical staff with special focus areas e.g., smart grid infrastructure.[94] The ITU Secretary-General submits a quarterly threat assessment to the UN Secretary-General. The organization maintains a database of experts as a resource base in case of a cyber-attack and shepherds the Global Cybersecurity Agenda.

From an international relations theory point of view, the ITU's role in the UN's activities regarding cyber-security is particularly notable because it is not only an organizational platform used by member states but also an autonomous norm entrepreneur. Its bureaucracy, namely its Secretary-General who considers cybercrime one of his top three priorities[95], acts beyond the traditional principal-agent relationship.

As an organizational platform and in line with classic principal-agent theory, the World Summit on Information Society in Tunis mandated the ITU to be responsible for Action Line C5 "Building confidence and security in the use of ICTs" confirmed by ITU plenipotentiary Resolution 140 (Rev. Antalya 2006).[96] In response to the Tunis agenda, the ITU Secretary-General, Hamadoun I. Toure, launched the Global Cyber-security Agenda in May 2007. A high-level experts group held three meetings between 2007 and 2008 before publishing its Global Strategic Report in 2008 which was later condensed into a 47-page brochure.[97] The Global Strategic Report focuses on five areas, (i) legal measures, (ii) technical and procedural measures, (iii) organizational structures, (iv) capacity building, and (v) international cooperation. The ITU

[92] UNIDIR "ICTs and International Security"
[93] CTITF May 2011: 7
[94] UN ITU *Global Strategic Report*, 2008: 95
[95] UN ITU "PowerPoint Presentation"
[96] Toure, 2011: 104
[97] UN ITU, March 2010

describes its Global Cyber-security Agenda to be an "international framework for cyber-security".[98]

The recommendations of the Global Cyber-security Agenda to the ITU include developing model legislation for member states to adopt and assisting in possibly using the Budapest Convention on Cybercrime as an example. Another recommendation is the creation of a "Cyber-security Readiness Index" based on organizational structures such as the existence of a national leader for coordination or national cyber-security council and the existence of a national CERT. It also proposes a framework for national infrastructure protection and suggests a conceptualization of what a culture of cyber-security as outlined in General Assembly resolution 57/239 could be understood to mean.[99] The Global Cyber-Security Agenda signed a memorandum of understanding with the International Multilateral Partnership against Cyber Terrorism (IMPACT) sponsored by the Government of Malaysia in 2008 which is considered the physical home of the Global Cyber-Security Agenda.[100] As aforementioned, the ITU also developed a tool kit for cyber-crime legislation with sample language including explanatory comments which could form the basis for a harmonization of cybercrime laws. It outlines a matrix comparing the legal provisions of laws in various countries.

As an autonomous norm entrepreneur, the ITU particularly stands out because of some of the actions taken by its Secretary-General. Generally, the ITU's strategy can be described as two-fold: firstly, it tries to advance the broad agenda set by its member states, and secondly, it focuses on specific initiatives. With regard to the latter, the Child Online Protection, for example, has been identified as an effort whose merit all states agree on and where trust can be built so that socialization effects could potentially produce positive spill over effects for the broader cyber-security agenda. In addition, at the 2010 World Telecom Development Conference in Hyderabad the Secretary-General proposed a "no first attack vow" for cyberspace and that states "should undertake not to harbour cyberterrorists and attackers in their country unpunished".[101] These remarks were only part of a speech and not an official request to member states. It is curious to note that Clarke and Knake have a similar proposal in their book *Cyberwar* stating that "the focus would be on keeping cyber attacks from starting wars, not on limiting their use once a conflict has started. We could apply the pledge to all nations or only to those nations that made a similar declaration or signed an agreement".[102]

At the same time, the ITU has not only served as an organizational platform for states. The World Federation of Scientists has played a particular noteworthy role in relation to the UN's and the ITU's activities relating to cyber-security. The World Federation of Scientists has also used the ITU as an organizational platform, albeit indirectly. In 2001, the Federation proposed a

[98] UN ITU, March 2010
[99] UN ITU, March 2010: see graphs on p. 76+121
[100] Toure, 2011: v
[101] The Hindu Business Line, 24 May 2010; Pradesh, 25 May 2010; Wegener, 2011: 81
[102] Clarke and Knake, 2010: 239

"universal order of cyberspace". Its August 2009 *Erice Declaration on Principles for Cyber Stability and Cyber Peace* explains the concept of cyber-peace further highlighting the free flow of information and ideas, a common code of cyber conduct and harmonized global legal framework, law enforcement efforts against cybercriminals, as well as developing more resilient systems. Most recently, the Chairman of the Federation's Permanent Monitoring Panel on Information Security, Henning Wegener, a retired German ambassador, wrote the chapter "Cyberpeace" in the 2011 publication *The Quest for Cyberpeace*.[103] Wegener openly acknowledges that the initiative is an "attempt to delegitimize cyberwar through reversing the perspective" while being "fully aware that digital infrastructures are now all-pervasive, and will unavoidably also be used for hostile, non-peaceful purposes".[104] (See the work of George Lakoff, professor of linguistics at the University of California, Berkeley, for a discussion on the importance of framing.[105]) He continues on to explain that "If the use of the term has more to do with politics and with political emphasis, with orienting the mind towards the right choices, then it follows that it must remain somewhat open-ended. The definition cannot be watertight, but must be rather intuitive and incremental in its list of ingredients".[106]

On the other hand, ITU's Secretary-General uses the World Federation of Scientists as an organizational role in his role as norm entrepreneur. The publication *The Quest for Cyberpeace*, for example, includes several contributions from ITU's Secretary-General.[107] His five principles for cyber peace are,

> "1. Every government should commit itself to giving its people access to communications.
>
> 2. Every government will commit itself to protecting its people in cyberspace.
>
> 3. Every country will commit itself not to harbor terrorists/criminals in its own territories.
>
> 4. Every country should commit itself not to be the first to launch a cyber attack on other countries.
>
> 5. Every country must commit itself to collaborate with each other within an international framework of co-operation to ensure that there is peace in cyberspace".[108]

The World Federation of Scientists fits the classic description of a norm entrepreneur according to Finnemore and Sikkink's definition that places value on altruism as motivation.[109] Its members clearly seem to be driven by altruistic intentions in the pursuit of peace. Its 1982 Erice Statement reads, "It is of vital importance to identify the basic factors needed to start an effective process to protect human life and culture from a third and unprecedented catastrophic war. To

[103] Wegener, 2011; World Federation of Scientists, 2003
[104] Wegener, 2011: 77
[105] Lakoff, 2006
[106] Wegener, 2011: 78
[107] Toure, 2011
[108] Wegener, 2011: 103
[109] Finnemore and Sikkink, 1998: 898

accomplish this it is necessary to change the peace movement from a unilateral action to a truly international one involving proposals based on mutual and true understanding".[110]

The Counter-Terrorism Implementation Task Force's Working Group on Countering the Use of the Internet for Terrorist Purposes

The Working Group on Countering the Use of the Internet for Terrorist Purposes can be considered to be an outlier in the network of UN organizations working on cyber-security. While it is now connected with the activities of the other organizations, its creation is not directly tied to the general discussions in the General Assembly on cyber-security. It is rather an anomaly because its creation took place in response to the 9/11 terrorist attacks and only later became linked to the broader cyber-security debate.

On September 28, 2001, the Security Council established the Counter-Terrorism Committee through resolution 1373 in response to the attacks on September 11. In 2004, the Security Council set up the Counter-Terrorism Committee Executive Directorate through resolution 1535 to oversee the implementation of resolution 1373. It currently consists of some 40 staff members.[111] The Counter-Terrorism Implementation Task Force (CTITF) was created by the UN Secretary-General in 2005 to ensure the coordination of the activities related to resolution 1373 and in 2009 within the Department of Political Affairs.[112] In 2006, the United Nations Global Counter-Terrorism Strategy was adopted, which includes a paragraph on exploring ways and means to "(*a*) Coordinate efforts at the international and regional levels to counter terrorism in all its forms and manifestations on the Internet; (*b*) Use the Internet as a tool for countering the spread of terrorism, while recognizing that States may require assistance in this regard".[113]

This is the basis for one of CTITF's working groups, the "The Working Group on Countering the Use of the Internet for Terrorist Purposes". Two UN staff members were mainly assisting this group in 2010, one at the Director and one at the Junior Professional Officer level. It has four goals: (i) identify and bring together stakeholders and partners on the abuse of the Internet for terrorist purposes, including using the web for radicalization, recruitment, training, operational planning, fundraising and other means, (ii) explore ways in which terrorists use the Internet, (iii) quantify the threat that this poses and examine options for addressing it at national, regional and global levels, and (iv) examine what role the United Nations might play.[114] It consists of

[110] World Federation of Scientists "The Erice Statement"
[111] UN Counter-Terrorism Committee
[112] UN CTITF "Main Page"
[113] UN General AssemblyA/RES/60/288
[114] UN CTITF "Working Groups"

The Monitoring Team of the 1267 Committee
CTITF Office
Alliance of Civilizations (joined at some point in 2010)
CTED
Department of Public Information
Interpol
Office of the High Commissioner for Human Rights
Special Rapporteur on Promotion and Protection of Human Rights While Countering
Unesco
United Nation Interregional Crime and Justice Research Institute
United Nations Office on Drugs and Crime

Type of Concern	Number of States Mentioning Concern
Cyberattacks	2
Fund-raising	4
Training	2
Recruitment	6
Secret	3
Data mining	3
Propaganda	Common
Radicalization	1

In February 2009, the Working Group published an initial report based on information provided by 31 member states[115] without disclosing the names of the countries. It collected information on the approaches taken by member states. The main conclusion of the report is that "there is not yet an obvious terrorist threat in the area" and that "it is not obvious that it is a matter for action within the counter-terrorism remit of the United Nations". It goes on to recommend that "If a more concrete threat of terrorist cyberattacks does materialize in the future, it might be a more appropriate and longer-term solution to consider a new international counter-terrorism instrument against terrorist attacks on critical infrastructure in general. It also highlights the distinction of the use of the Internet for terrorist purposes between terrorism-specific gaps and internet-specific gaps. Moreover, the definition of critical infrastructure could, if necessary, be updated (perhaps by protocol to the treaty) to include information infrastructure, if this becomes important." And that "counter-narrative works holds exciting promise, but is still in its infancy and requires further exploration".[116]

The report groups the use of the Internet for terrorist purposes into four types

(i) To perform terrorist attacks by remotely altering information on computer systems or disrupting the flow of data between computer systems;

(ii) As an information source for terrorist activities;

[115] Afghanistan, Algeria, Australia, Austria, Belarus, Belgium, Bosnia and Herzegovina, Canada, Finland, Germany, Iceland, Japan, Jordan, Saudi-Arabia, Malta, Morocco, the Netherlands, New Zealand, Nigeria, Norway, Oman, Pakistan, Poland, Portugal, Russia, Senegal, Serbia, Spain, Switzerland, the United Kingdom and the U.S.
[116] UN CTITF, February 2009: 26

(iii) Means for disseminating content relevant to the advancement of terrorist purposes;

(iv) Means for supporting communities and networks dedicated either to pursuing or supporting acts of terrorism

The report outlines that member states suggested the following ways the UN could further contribute through

(i) Facilitating member states sharing of best practices

(ii) Building a database of research into use of the Internet for terrorist purposes

(iii) More work on countering extremist ideologies

(iv) Creation of international legal measures aimed at limiting the dissemination of terrorist content on the Internet

A second report focusing on the legal and technical challenges was published in May 2011. It builds on the first and is based on a meeting organized by the German Foreign Ministry in Berlin in January 2010 and one hosted by Microsoft in Redmond, Washington in February 2010. The section on legal aspects highlights that there have been three trends

(i) Some countries apply existing cybercrime legislation to terrorist use of the Internet;

(ii) Some countries apply existing counter-terrorism legislation to Internet-related acts; and

(iii) Some countries have enacted specific legislation on terrorist use of the Internet.[117]

Moreover, it distinguishes laws that are Internet-specific and those that are not. For example, Article 10 of the Russian Federal Law 149-FZ of July 27, 2006 on Information, Information Technologies and Protection of Information is not Internet specific. China's Article 5 of the Chinese Computer Information Network and Internet Security, Protection and Management Regulations on the other hand is an Internet-specific approach to regulating the issue legally.

The report also highlights that the 9/11 attacks broadened the understanding of how the Internet can be used by terrorists. It calls for a harmonization of national legislations by implementing regional instruments such as the Budapest Convention on Cybercrime or the Commonwealth Model Law on Cybercrime as well as international instruments such as the Convention against Transnational Organized Crime. The section on technical aspects is more of a compendium on the technological possibilities and past cases of abuse.

A third report is in the making after the Working Group began focusing on using the Internet for counter-narratives to terrorism in 2011 including a major conference in Saudi Arabia in January.[118] An in-depth study of the issue is expected to be published in the latter half of 2011.[119]

[117] UN CTITF, report May 2011: ix
[118] UN CTITF "Working Group on Countering the Use of the Internet for Terrorist Purposes"
[119] UN CTITF, May 2011: vii

II.2. The Economic Stream: Cyber-crime

The governance structure on crime at the United Nations is even more complex than is typical of the UN system. So, a few explanatory remarks to start. The General Assembly, the plenary of UN member states, has been dealing with the issue as well as ECOSOC with its smaller membership of only 54 out of the 193 UN member states. In addition to ECOSOC with its 54 members, two of its functional commissions focus on crime: the Commission on Narcotic Drugs and the Commission on Crime Prevention and Criminal Justice. Both meet annually. They are the governing body of UNODC, the UN's bureaucratic apparatus focusing on crime.[120] Lastly, in addition to the aforementioned bodies, an independent United Nations Congress on Crime Prevention and Criminal Justice takes place every five years. This congress makes recommendations to the Commission on Crime Prevention and Criminal Justice. My analysis starts with the General Assembly, then proceeds to examine the negotiations linked to ECOSOC, and finishes with an analysis of the UNODC as an organizational platform.

II.2.1. The Third Committee of the General Assembly and ECOSOC

The Third Committee focusing on the "criminal use of information technologies"[121]

Two years after the Russian Federation introduced the resolution in the First Committee, the Third Committee - Social, Humanitarian, and Cultural - discussed a draft resolution entitled "Combating the criminal misuse of information technologies" (A/55/59, 16 November 2000) as part of its work on crime prevention and criminal justice. It was introduced by the United States and 38 other member states including the Russian Federation, France, Israel, and the United Kingdom with another 19 member states subsequently cosponsoring it. The People's Republic of China did not co-sponsor the resolution.[122] The draft resolution was adopted without a vote on January 22, 2001.

The key objective of Resolution 55/63 is to establish a "legal basis for combating the criminal use of information technologies". [123] The resolution refers to the precedent set in 1990 when the Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders adopted a resolution on computer-related crimes. It also notes the work of the Council of Europe on the Budapest Cybercrime Convention. The resolution's key elements are

- "recognizing that the **free flow of information** can promote economic and social development, education and **democratic governance** […]
- "Expressing concern that technological advancements **have created new possibilities for criminal activity**, in particular the criminal misuse of information technologies […]"

[120] UNODC "Secretariat to the Governing Bodies Section"
[121] UN General Assembly A/RES/55/63
[122] UN General Assembly A/55/593
[123] UN General Assembly A/57/529/Add. 3

- "recognizing the need for cooperation between States **and private industry** in combating the criminal misuses of information technologies […]"

- "The fight against the criminal misuse of information technologies requires the development of solutions taking into account both the protection of individual freedoms and privacy and the preservation of the capacity of Governments to fight such criminal misuse" [emphasis made by the author].[124]

In 2001, a follow-up resolution was introduced by the United States and 73 other member states including the Russian Federation, France, Israel, the Republic of Korea, and the United Kingdom with 8 member states joining later. The draft resolution was adopted on without a vote on January 23, 2002. The People's Republic of China did not co-sponsor the resolution.[125] This resolution, 56/121, summed up the objective of its predecessor as inviting "Member States to take into account measures to combat the criminal misuse of information technologies". Its draft was changed with the second preambular paragraph ultimately reading "democratic governance" rather than "democracy and good governance".

Importantly this 2002 resolution concludes by stating that the Committee "decides to defer consideration of this subject, pending work envisioned in the plan of action against high-technology and computer-related crime of the Commission on Crime Prevention and Criminal Justice".[126] This decision has effectively moved the substantive cyber-crime related discussion out of the General Assembly to the Commission on Crime Prevention and Criminal Justice, one of ECOSOC's functional commissions and one of the intergovernmental bodies of UNODC as explained in the section on UNODC below.

The only further activity of the Third Committee on the issue of cyber-crime is contained in GA resolutions 63/195 (2008), 64/179 (2009), and 65/232 (2011) titled "Strengthening the United Nations Crime Prevention and Criminal Justice Programme, in particular its technical cooperation capacity". They simply "draw attention to […] the issue of cyber crime, and invites the United Nations Office on Drugs and Crime to explore, within its mandate, ways and means of addressing these issues".[127] Their predecessor, resolution 62/175 referenced "identity theft" which was expanded for the first time in resolution 63/195 to also mention the term "cyber-crime". The sponsorship of these resolutions has been led by Italy.[128] The latest in this series of resolutions, resolution 65/232, no longer references "identity theft" but "notes with appreciation the convening of an open-ended intergovernmental expert group to conduct a comprehensive study of the problem of cybercrime".[129]

[124] UN General Assembly A/RES/55/63
[125] UN General Assembly A/56/574
[126] UN General Assembly A/RES/56/121
[127] UN General Assembly A/RES/63/195; A/RES/64/179; A/RES/65/232
[128] UN General Assembly A/63/431; UN General Assembly A/64/440; UN General Assembly A/65/457
[129] UN General Assembly A/RES/65/232

With regard to the Twelfth United Nations Congress on Crime Prevention and Criminal Justice, the General Assembly in resolution 63/193, approved as an agenda item "Recent developments in the use of science and technology by offenders and by competent authorities in fighting crime, including the case of cybercrime"[130] Resolution 65/230 includes a request to include cyber-crime in UNODC's technical assistance programs and capacity building.[131]

This makes the First Committee the only committee in the General Assembly that continues to focus on cyber-security norms substantively up to date.

The Commission on Crime Prevention and Criminal Justice

The first session of the Commission on Crime Prevention and Criminal Justice took place in 1992. It was not until 2010 that cybercrime occurs as a prominent theme in its annual reports. The report on the Commission's third session in 1994 makes a first reference that technical cooperation regarding "computer crime" was considered inviting the Ninth Congress to look at the issue.[132] (This early activity builds on the work of the Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders in 1990 and its resolution on computer-related crimes.) In 1998, the Commission eventually asked the General Assembly to include in the agenda of the Tenth Congress a workshop on "crimes related to the computer network". In 1999, the Commission proposed a draft resolution for ECOSOC on the "Work of the United Nations Crime Prevention and Criminal Justice Programme" requesting the Secretary-General to conduct a study on computer-related crimes and to report on his results at its tenth session. It also mentions an expert meeting on crime relating to computer networks in Japan in 1998. Yet, the 2000 report does not mention the terms "cyber", "Internet", nor "identity", while including only one reference to "technology" and three references to "computer". A similar pattern occurred in 2001.

The report of 2002 mentions the term "cyber" for the first time, using it twice, and also makes reference to the Convention on Cybercrime. The report in 2003 again makes no mention of "cyber" nor of "technology" and "identity". The term "Internet" is mentioned three times and "computer" only once in reference to the suggestion of the 2002 report to include a workshop on "measures against high-technology and computer-related crime" for the Eleventh Congress though. The first recorded call for a United Nations Convention against cybercrime appears in the 2004 report mentioning that one speaker made such a suggestion with regard to the Eleventh Congress. The report also includes a first draft resolution for ECOSOC on "International cooperation in the prevention, investigation, prosecution and punishment of fraud, the criminal misuse and falsification of identity and related crimes" (see section on ECOSOC for further

[130] UN General Assembly A/RES/63/193; UN General Assembly A/63/431
[131] UNODC "Open-ended intergovernmental expert group"
UN General Assembly A/RES/65/230; UN ECOSOC E/2011/30
[132] UN ECOSOC E/1994/31: 65

analysis). The 2005 and 2006 reports make several references to the aforementioned terms but without taking further action. The 2007 report includes again a draft resolution for ECOSOC on "International cooperation in the prevention, investigation, prosecution and punishment of fraud, the criminal misuse and falsification of identity and related crimes" as in 2004 (see section on ECOSOC for further analysis). In 2008, the Commission decides to include "economic fraud and identity-related crime" as one of two thematic discussion of the Twelfth Congress and as well as an agenda item on "Recent developments in the use of science and technology by offenders and by competent authorities in fighting crime, including the case of cybercrime".

In 2009, the Commission held thematic discussions on economic fraud and identity-related crime and prepared a draft resolution for adoption by ECOSOC on "International cooperation in the prevention, investigation, prosecution and punishment of economic fraud and identity-related crime", which describes the Convention on Cybercrime as "currently the only international treaty specifically addressing computer-related fraud, computer-related forgery and other forms of cybercrime that may contribute to the perpetration of economic fraud, identity-related crime, money-laundering and other related illicit activities" (see section on ECOSOC for further analysis). Its draft decision for ECOSOC for the "Report of the Commission on Crime Prevention and Criminal Justice on its eighteenth session and provisional agenda and documentation for its nineteenth session" outlines the decision that "the prominent theme for the twentieth session of the Commission will be 'Protecting children in a digital age: the misuse of technology in the abuse and exploitation of children' ".[133]

The 2010 report mentions that some speakers brought up a global convention against cybercrime again. It also includes a draft resolution by the Commission for ECOSOC to be adopted by the General Assembly to request the Commission - yes, it is a circular process - to establish

> "an open-ended intergovernmental expert group, to be convened prior to the twentieth session of the Commission, to conduct a comprehensive study of the problem of cybercrime and responses to it by Member States, the international community and the private sector, including the exchange of information on national legislation, best practices, technical assistance and international cooperation, with a view to examining options to strengthen existing and to propose new national and international legal or other responses to cybercrime".[134]

The 2011 report has by far the most numerous references to "cyber" so far. It includes resolution 20/7 brought to the attention of ECOSOC, titled "Promotion of activities relating to combating cybercrime, including technical assistance and capacity-building". It highlights that the Convention against Transnational Organized Crime can be used against cybercrime in the context of organized crime. It also includes a draft resolution for ECOSOC titled "Prevention, protection and international cooperation against the use of new information technologies to abuse

[133] UN ECOSOC E/2009/30
[134] UN ECOSOC E/2010/30; UN ECOSOC resolution 2010/18; UN General Assembly A/RES/65/230

and/or exploit children" mentioning cyberbullying for the first time. Another draft resolution on "International cooperation in the prevention, investigation, prosecution and punishment of economic fraud and identity related crime" requests UNODC to continue its work on identity related crime and to use data of intergovernmental group for work on children as well as recommending to the expert group to take into account work of group of experts on identity related crime as well as mentioning UNODC's Handbook on Identity-related Crime Government of Canada financial support.

The Commission on Narcotic Drugs on the Internet and drug trafficking

The Commission on Narcotic Drugs predates the Commission on Crime Prevention and Criminal Justice. It has focused on the role of the Internet relating to crime with regard to drug trafficking as early as 1996 during its 39th session.[135] Interestingly, one of the earlier documents focuses mostly on the potentially positive uses of the Internet in drug control.[136] In 1999, the report on its annual session included a chapter on "the impact of communication networks, such as the Internet, on the drug problem".[137] In 2000, the Commission eventually adopted a resolution solely focused and titled "Internet" which was brought to the attention of ECOSOC. Unlike earlier documents this resolution highlights how the World Wide Web is (mis)used for advertising and sale of illicit drugs. It was sponsored among others by the U.S. but not by Russia or China.[138] After 2000, there has not been a specific resolution on the Internet but repeated references to it as part of the Commission's discussions.

In 2004, in reference to the 2000 resolution, the Commission prepared a draft resolution for ECOSOC, which was adopted as ECOSOC resolution 2004/42 on the "Sale of internationally controlled licit drugs to individuals via the Internet".[139] The draft was co-sponsored by the U.S. but not Russia or China. In 2005, the Commission adopted a new resolution, this time titled "Strengthening international cooperation in order to prevent the use of the Internet to commit drug-related crime," which was co-sponsored, among others, by the U.S. and Russia, but not China and brought to the attention of ECOSOC.[140] A similar resolution co-sponsored by the U.S. but not Russia or China was adopted in 2007 on "International cooperation in preventing the illegal distribution of internationally controlled licit substances via the Internet" making reference to resolution 43/8 and was also brought to the attention of ECOSOC.[141] Ultimately, however, the Commission on Narcotic Drugs has focused on the Internet only from a drug trafficking perspective in line with its functional mandate.

[135] UN ECOSOC E/1999/28/Rev.1: p .45
[136] UN General Assembly A/RES/S-20/4
[137] UN ECOSOC E/1999/28/Rev.1
[138] UN ECOSOC resolution 43/8 in E/2000/28
[139] UN ECOSOC E/2004/28
[140] UN ECOSOC resolution 48/5 in E/2005/28
[141] UN ECOSOC resolution 50/11 in E/2007/28/Rev. 1

The Economic and Social Council on identity-related crimes

ECOSOC, in turn, adopted a resolution on identity-related crimes for the first time in 2004. Resolution 2004/26 on "International cooperation in the prevention, investigation, prosecution and punishment of fraud, the criminal misuse and falsification of identity and related crimes" focused on member states and expressed a concern that "the spread of modern information and communication technologies creates a vast range of new opportunities for fraud and the criminal misuse and falsification of identity".[142] It also requests the Secretary-General to convene an intergovernmental expert group to prepare a study on fraud and the criminal misuse and falsification of identity. The group and its meetings were supported by the governments of Canada and the United Kingdom.[143]

Its successor, resolution 2007/20, notes the "Council of Europe's Convention on Cybercrime, which is an international legal instrument open to ratification or accession by States not members of the Council" encouraging "member states to consider acceding" to it. It also "Requests the United Nations Office on Drugs and Crime to provide, upon request and subject to the availability of extrabudgetary resources, legal expertise or other forms of technical assistance to Member States".

The last in this series of resolutions, resolution 2009/22, elaborates on its request to UNODC and makes reference to the report of this expert group. It also states that

> "For the above-mentioned reasons, the United Nations Convention against Transnational Organized Crime, the United Nations Convention against Corruption and, where applicable, the Council of Europe Convention on Cybercrime, as well as the 13 universal legal instruments against terrorism, appear to provide a more than adequate framework and legal basis for the types of mutual legal assistance, extradition and other forms of international cooperation that are needed to deal with transnational cases of economic fraud and identity-related crime. As a result, the Intergovernmental Expert Group saw no need for any further international legal instruments in that area" instead pointing out to member states to ratify those instruments if they had not yet done so.[144]

The resolution also outlines the follow-up to the work of the expert group and

> "Acknowledges the efforts of the United Nations Office on Drugs and Crime to establish, in consultation with the United Nations Commission on International Trade Law, a core group of experts on identity-related crime and bring together on a regular basis representatives from Governments, private sector entities, international and regional organizations and academia to pool experience, develop strategies, facilitate further research and agree on practical action against identity-related crime".[145]

[142] UN ECOSOC resolution 2004/26
[143] UN ECOSOC resolution 2009/22; UN ECOSOC E/CN.15/2009/2 and Corr.1
[144] UN ECOSOC E/CN.15/2007/8 and Add.1-3
[145] UN ECOSOC E/CN.15/2007/8 and Add.1-3

This group has been established and has met several times. The publication of the results of this expert group took place shortly before the Twelfth United Nations Congress on Crime Prevention and Criminal Justice - the first since 2005. As aforementioned, its agenda included cybercrime. However, states participating in the Twelfth United Nations Congress on Crime Prevention and Criminal Justice in Salvador, Brazil, in April 2010 did not come to an agreement on a cyber-crime treaty.[146] This ongoing debate mainly centers on the question whether the Budapest Convention on Cybercrime originally adopted by the Council of Europe will become a global convention or a "regional initiative" as it was recognized by the World Summit of the Information Society.[147]

The U.S. ratified the treaty but Russia refuses to do so as long as it condones cross-border searches by foreign law enforcement agencies as previously stated in this paper. Instead, the Congress's outcome document invites the Commission on Crime Prevention and Criminal Justice to establish a new open-ended intergovernmental expert group

> "to conduct a comprehensive study of the problem of **cybercrime** and responses to it by Member States, the international community and the private sector, including the exchange of information on national legislation, best practices, technical assistance and international cooperation, with a view to examining options to strengthen existing and to propose new national and international legal or other responses to **cybercrime** [emphasis by the author]".[148]

The group met in Vienna from January 17-21, 2011, with representatives from 78 member states attending. The meeting report includes a list of topics and the methodology for the study submitted to the Commission at its twentieth session in Vienna from April 11-15, 2011, as requested in paragraph 11 of resolution 65/230 (see E/CN.15/2011/19 for the list of topics and scope of study). The General Assembly "noted with appreciation the convening" of the group in its resolution 65/232.[149]

II.2.2. Organizational Platforms: UNODC and UNICRI

The United Nations Office on Drugs and Crime

UNODC has a relatively big budget compared to the other UN organizations discussed in this paper, but has only one staff member working full-time on cyber. (This staff member previously served at UNICRI.) The first requests for UNODC to become involved in technical assistance specifically relating to "cyber-crime" date back to the Third Committee and GA resolution 63/195 of 2008. In response, UNODC held a first one-week training workshop on cybercrime for

[146] Toure, 2011: 92
[147] UN ITU *Global Strategic Report*, 2008: 14
[148] UN General Assembly A/CONF.213/18
[149] UN General Assembly A/RES/65/232

law enforcement officers in June 2009.[150] Moreover, UNODC's Terrorism Prevention Unit has been contributing to a CTITF publication for law enforcement investigators and criminal justice officers on cases involving the use of the Internet for terrorist purposes to be released in early 2012. Member state officially requested UNODC to work on the use of the Internet for terrorist purposes for the first time at the 20th session of the Commission on Crime Prevention and Criminal Justice in April 2011[151] after it was first mentioned at the 19th session the year before.[152] The ITU's cyber law tool kit is similar to the UNODC tool kit model and its public database of national legislation is a unique resource for legal analyses.

The United Nations Interregional Crime and Justice Research Institute

The United Nations Interregional Crime and Justice Research Institute in Turin, Italy, is among the smaller players in the UN system. It is research focused and mandated to assist intergovernmental, governmental and non-governmental organizations in formulating and implementing improved policies in the field of crime prevention and criminal justice. It produces the magazine *F3 – Freedom From Fear* together with the German Max Planck Institute and the Swiss Basel Institute on Governance. Its last issue, number 7, focused on cyber security.

From a cyber-security point of view, UNICRI's particular strength is that Raoul Chiesa, a former hacker with technical expertise, supports the institute on a pro bono basis as a consultant. He has been a driving force of the Hackers Profiling Project. In 2008, the project members published a book titled *Profiling Hackers – The Science of Criminal Profiling as Applied to the World of Hacking*. One of its outstanding contributions is its attempt at a typology for actors in cyber-space. They identify Wannabee Lamer; Script-kiddie; the "37337 K-rAd iRC #hack 0-day exploitz" guy; Cracker; Ethical Hacker; Quiet, paranoid, and skilled hacker; Industrial Spy; Cyber-warrior; Government Agent, Military Hacker. [153] As these types sometimes overlap, they can be reduced to the following three groups relevant in cyber-warfare:

Cyber-warrior: private actors who are highly skilled mercenaries hacking for money or for ideals including criminals and terrorists

Government Agent: "the civilian state actor" - hackers employed by a country's civilian government for (counter)espionage, information monitoring of governments, terrorist groups, strategic industries, and individuals without the authority to cause physical death through the use of the electronic world[154]

[150] UNODC "Law enforcement officers trained"
[151] UN ECOSOC E/2011/30
[152] UN ECOSOC E/2010/30
[153] Chiesa et al, 2009: 52-56, 61
[154] Chiesa et al, 2009: 56

Military Hacker: "the military state actors" - hackers employed by a country's military potentially with the authority to cause physical death through the use of the electronic world in times of war

This categorization is more elaborate than Clarke and Knake's general usage of the term cyber warriors which simply distinguishes between criminals and military hackers. The UNICRI-based categories provide greater clarity to differentiate between the various actors in cyber-warfare, state and non-state as well as military and civilian. (UNICRI's *Profiling Hackers – The Science of Criminal Profiling as Applied to the World of Hacking* also provides an overview of the different techniques of hacking.[155]) This is a particularly helpful contribution because the various actors operating in cyber-space are often not differentiated properly in media and sometimes scholarly texts. Mixing and considering juvenile teenagers engaged in webdefacing on par with the creators of Stuxnet only contributes to what some perceive a hype.[156]

In 2010, UNICRI contributed to developing the guidelines for the ITU's Child Online Protection Initiative.[157]

II.3. The Second Committee of the General Assembly – "A global culture of cyber-security"

The three resolutions of the General Assembly's Second Committee on "a global culture of cyber-security" link the two streams – politico-military and economic - referencing the resolutions of both the First and Third Committee.[158]

After the decision of the Third Committee to no longer focus on cyber-crime, the United States introduced a new draft resolution in 2002, this time in the Second Committee—Economic and Financial—entitled "Creation of a global culture of cyber-security". This was embedded in the ongoing discussion on "Macroeconomic policy questions: science and technology for development".[159] It was introduced also on behalf of Japan, and Australia and Norway joined in co-sponsoring the original draft. After a number of revisions an additional 36 member states co-sponsored the draft resolution including the Russian Federation, France, and the Republic of Korea. The final resolution text (A/RES/57/239) also includes references to the resolutions adopted in the First Committee after revisions to the draft. It was adopted without a vote. The People's Republic of China did not co-sponsor the resolution.[160] (Unfortunately the statements of the U.S. representative and four other member states after the adoption of the resolution is not noted in the document A/C.2/57/SR.44 cited as reference in the Committee's report A/57/529/Add.3.) The three key changes to the original draft are:

[155] Chiesa et al, 2009: 20-32
[156] Singer, 2011
[157] UNICRI "Cybercrimes"
[158] UN General Assembly A/RES/57/239; A/RES/58/199; A/RES/64/211
[159] UN General Assembly A/57/529/Add. 3
[160] UN General Assembly A/57/529/Add. 3

- First, the inclusion of a paragraph noting "gaps in access to and the use of information technologies by States can diminish the effectiveness of international cooperation in combating the criminal misuse of information technology". The key argument of this paragraph is the known and regular call by developing countries for a "transfer of information technologies, in particular to developing countries". This point, together with the need for capacity-building is reiterated in the last operative paragraph of the resolution and is likely to have been the negotiated compromise for member states from developing countries to agree to an adoption of the draft resolution. An explanation for the apparent contradictory statement of this sentence – if there are gaps in access, then those gaps also affect the criminal misuse – could be that there might be gaps in access by States but not necessarily by criminals in those States.

- Second, changing the original wording of "Adopts the principles annexed to the present resolution" to "Takes note of the elements" representing a watering down of the original language due to the change of "principles" to the weaker "elements" and usually the order of terminology being adopt/welcome/notes with appreciation/takes notes/ acknowledges. A global culture of cyber-security according to these "elements" is said to require nine complementary elements: awareness, responsibility, response, ethics, democracy, risk assessment, security design and implementation, security management, and reassessment (see appendix). Despite the change of the wording these elements can be seen as a first attempt of a consensus on basic international principles and signs of norm emergence.

- Third, the final resolution only "invites" rather than "requests" member states to take the resolution into account for the World Summit on the Information Society held in Tunis in 2005 with input from private sector and civil society. The Tunis summit counted 1500 participants from international organizations, 6200 from nongovernmental organizations, 4800 from private sector and 970 media representatives.

The second resolution on a global culture of cyber-security negotiated in 2004 and adopted by the General Assembly in January 2005 is expanded to include the protection of critical information infrastructures outlining key elements in an annex (see appendix). These elements are based on the 2003 meeting of the G8 Ministers of Justice and Interior. This link is another sign of how the various internationally agreed upon elements and principles states are starting to form a web possibly thickening to a regime.[161] Interestingly, the resolution no longer contains a reference to the dependence on governments on new technologies but the link between countries' critical infrastructures and countries' critical information infrastructures. It was cosponsored by a total of 69 countries including China but not Russia.[162] Compared to the first draft, the final text (resolution 58/199) includes a new preambular paragraph stating "that each country will

[161] UN ITU *Global Strategic Report*, 2008: 24
[162] UN General Assembly A/58/481/Add.2

determine its own critical information infrastructure". It also includes a new operative paragraph encouraging member states to share best practices.

The third resolution, resolution 64/211, was adopted in 2010 after the U.S. policy shift. The second part of its title "Creation of a global culture of cybersecurity and taking stock of national efforts to protection critical information infrastructures" reveals the important piece of the document. It includes an annex (see appendix) outlining a "Voluntary self-assessment tool for national efforts to protect critical information infrastructures" with a detailed road map for member states. It was sponsored by the U.S. on behalf of 39 other countries. Russia and China did not co-sponsor this resolution. The key changes to the original draft are:

- First, references to civil society and business were taken out of the original draft of the resolution text itself. The section mentioning "freedom of expression and the free flow of information, ideas and knowledge" was also deleted" as well as the suggestion to submit relevant information by a set deadline, by the sixty-fifth session.

- Second, the final text emphasizes the "importance of the mandate of the Internet Governance Forum" and "reiterating that all Governments should have an equal role and responsibility for international Internet governance" relating to the larger Internet governance debate. It also highlights "that each country will determine its own critical information".

- Third, the resolution highlights the importance of "international information-sharing and collaboration, so as to effectively confront the increasingly transnational nature of such threats" and encourages member states to share best practices for dissemination.

There were only minor edits to the language in the annex.

III. The Internet Governance Forum

The creation of the Internet Governance Forum is based on Paragraph 72 of the Tunis Agenda, the outcome document of the second phase of the World Summit on the Information Society from November 16-18, 2005. Member states took two important decisions regarding the UN and cyber. First, they asked the UN Secretary-General to create the IGF, the focus of this section.[163] Second, the ITU is given the responsibility for Action Line C5 "Building confidence and security in the use of ICTs" as discussed above.[164] (On a side note, the outcome document of the summit reaffirms UNGA resolution 57/239 on the culture of cyber-security but does not mention the protection of critical information infrastructure despite the invitation in GA resolution A/RES/58/199. It does make reference to the resolutions on the criminal misuse of information technologies though.[165])

A battle took place at the 2005 World Summit on Information Society.[166] It was a battle among governments over the domain name governance that has been carried out by ICANN. ICANN, firmly controlled by Americans, has been viewed with suspicion by governments who would like to have a say. In 2010 for example the Chinese government wrote in its white paper on Internet policy that "China holds that the role of the U.N. should be given full scope in international Internet administration".[167] In Tunis, some members of the European Union supported a push for an intergovernmental group to replace ICANN. The U.S. eventually compromised and the IGF was created as a forum "in which governments could debate and make recommendations about Internet policy issues but not exercise direct policy authority. The Tunisia compromise is the latest round in the battle for control of the Internet's naming system – a battle in a larger war for control over the Internet. It is too early to say who will win this war".[168] (See Zittrain pp. 242+243 for a critical analysis of the IGF and the domain name governance debate as well as Wu and Goldsmith 2008: 41-42 for an earlier episode of the debate.)

The IGF has since been dependent on voluntary contributions with its head reporting to the Under-Secretary General of the Department of Economic and Social Affairs, currently Sha Zukang from China. Its staff consists of its Executive Coordinator (Markus Kummer, 2006-2011[169]), a Programme and Technology Manager, and two part-time consultants.[170] The IGF's recommendations are submitted to the UN Secretary-General who, in turn, submits them to the General Assembly. (For an assessment of future developments see Kieren McCarthy.[171])

[163] UN World Summit on the Information Society, 2005: 17
[164] UN World Summit on the Information Society, 2005: 26
[165] UN World Summit on the Information Society, 2005: 13
[166] Wu and Goldsmith, 2008: 171
[167] Ford, 2010: 65
[168] Wu and Goldsmith, 2008: 171
[169] UN Internet Governance Forum "Past Staff Members"
[170] UN Internet Governance Forum "About IGF"
[171] McCarthy, 2011

Conclusion

The activities at the United Nations show clear signs of nascent cyber norms slowly emerging. Key evidence in support of this assessment is the number of General Assembly resolutions adopted over time in various committees, the annexed elements, the increasing number of co-sponsors, and the requests for bureaucracies to become involved in the issue and deliver technical assistance particularly after 2005. Moreover, a new Group of Governmental Experts will form in 2012 to submit a report in 2013, marking the next step in the politico-military stream and the norm emergence process.

However, my analysis of the two streams also shows that the process of norm emergence is dynamic. I outline how the negotiations in each one of them are connected with one another, reinforcing and building on previous developments. I identify how the dynamic in a norm life cycle at the international level seems to depend on (i) the overall relationship between actors with changes in that relationship also changing because of domestic conditions including the change of an administration and (ii) exogenous factors altering the perceptions among senior policy makers such as the cyber incidents that started making major headlines in 2007.

Russia has been playing a crucial role in this process with the U.S. as the most important counterweight. Germany, Canada, and the United Kingdom have also played an active role funding various research projects and expert groups. Curiously, China seems to have been rather inactive except for its co-sponsorship of the resolution in the First Committee in the year after the U.S. decided to vote against it for the first time and the recent code of conduct.

This paper shows that states play an important role as norm entrepreneurs. While their motives are arguably primarily driven by their own interests and a logic of consequences, the latter do not need to exclude altruistic motives and a logic of appropriateness to be influential, as well. As scholars Peter A. Hall and Rosemary C.R. Taylor have already pointed out, the two are not mutually exclusive.[172] This is underlined when one reads the arguments made by officials of the Russian government. For example, Komov, Korotkov and Dylevski as well as Streltsov make numerous references to the UN Charter and substantiate his line of reasoning with moral arguments.[173]

The UN system itself is rather fragmented in its activities regarding cyber-security. Individual organizations are used as organizational platforms by states to further their own agenda. Nevertheless, some significant work is being done. Reports of the Working Group on the Use of the Internet for Terrorist Purposes, for example, reveal some interesting and rare data on states' perception of the cyber-security threat (in spite of the fact that the reports do not identify specifically which information was submitted by what state). Moving forward from an organizational theory point of view, the question will be how to use the expertise and efforts of

[172] Hall and Taylor, 1996
[173] Komov et al, 2007; Streltsov, 2007

the various initiatives best while trying to avoid pitfalls of the past and potentially adopting more network like structures given the small number of staff and geographic disparity.

There are even some unanticipated consequences that can be identified. The ITU's active support of the cyber-peace initiative pushed by the World Federation of Scientists arguably goes beyond what its principals (i.e. member states) likely intended when they tasked the organization with Action Line C5 at the Tunis Summit After all, the Federation's principles include the plea that "All governments should make every effort to reduce or eliminate restrictions on the free flow of information, ideas and people. Such restrictions add to suspicion and animosity in the world" as outlined in its 1982 Erice Statement. This would rule out previous efforts by the Russian government to use the Internet to control the flow of information as highlighted by Ford.

In terms of next steps for future research and further questions, the following four themes are only the beginning of a list and surely not exhaustive:

First, several member states sent various statements to the UN Secretary-General as a result of the work in the First Committee in which they outline their positions and views on cyber-security. There seems to be a wealth of information for a more comprehensive picture on how countries across the globe think about this issue and how their thinking evolved over time. Was the U.S. policy shift a tactical move or a strategic one with long-term consequences? More generally, the complex question of lines of authority also emerges. For example, the U.S. State Department is the official representation of the U.S. government at international organizations. Should the Department of Defense or the Department of Commerce sit at the table when dealing with cyber-security? What is the role of Chris Painter in the new position as Coordinator for Cyber Issues at the State Department? How do the Russian Ministry of Foreign Affairs and Defense Ministry coordinate their positions at the ITU, for example? What about the Chinese government?

Second, future in-depth analyses of the activities at each UN suborganization could expand the often limited and sometimes merely descriptive accounts of this paper. Particularly noteworthy are anecdotes suggesting that certain states use certain UN organizations as organizational platforms. For example, the claims that UNODC is an "American" influenced organization, whereas the ITU is under the influence of "Russia and China". Such claims tend to reference the nationality or place of education of the head of the organization or else are assumed based on the primary sources of the organization's funding. For example, ITU's current Secretary-General, Hamadoun Toure, received his university education in Russia[174], or main financiers as indicators. This is a point worthy of further inquiry to shed light on how an organization is exactly used by a norm entrepreneur and perhaps by various norm entrepreneurs at the same time.

Third, the UN is only one player in the world of multilateralism. An obvious question is how the activities at the UN in New York, Geneva, and Turin are linked to activities at the European

[174] Toure, 2011: viii-ix

Union and NATO in Brussels, the OECD in Paris, or ASEAN in Jakarta similar to how the interactions in the three General Assembly committees influenced each other. My analysis already highlighted two of those linkages with regard to the principles adopted by the G8 and the Budapest Convention on Cybercrime based on the Council of Europe.

Fourth, with first signs of norm emergence occurring in the past decade, will a cascade occur? The process is dynamic so when and why do ups and downs occur? My analysis has already identified an obvious one rooted in the domestic political environment of one member state and the change of administration. However, this could also be understood to be only the symptom of larger trends. What other factors influence the rise and decline of norms and under what conditions? How have outside norm entrepreneurs such as the World Federation of Scientists influenced the process exactly and are they likely to continue to do so possibly joined by others as a result of a greater awareness? Moreover, are emergent norms spill-overs from existing norm systems relating to criminal or military activity which are modified to apply to cyberspace or are they entirely new norms?

In short, research on cyber-security and international relations is still in its infancy. With every new paper, more questions are likely to be raised than answered. While many of the debates were still in the realm of science fiction when Russia introduced the first draft resolution in 1998, Stuxnet has signaled that fiction has turned into science. An official consensus has not been reached on basic definitions of cyber-security since the first attempt to do more than a decade ago. Yet, the activity of the past decade exhibits an astonishing rate of norm emergence in cyber-space relative to typical international relations timelines.

Works Cited

Literature

Abbott, Kenneth W., and Duncan Snidal. "Hard and Soft Law in International Governance." *International Organization* 54.3 (2000): 422.

Barnett, Michael N., and Liv Coleman. "Designing Police: Interpol, and the Study of Change in International Organizations." *International Studies Quarterly* 49 (2005): 593-619.

Barnett, Michael and Martha Finnemore. "Rules for the World – International Organizations".in *Global Politics*. New York: Cornell University Press, 2004.

Barnett, Michael and Martha Finnemore. "The Politics, Power, and Pathologies of International Organizations." *International Organization* 53.4 (1999): 699-732.

Boyle, Alan E. "Some Reflections on the Relationship of Treaties and Soft Law." *The International and Comparative Law Quarterly* 48.4 (1999): 901-02.

Broad, William J., John Markoff and David E. Sanger. "Israeli Test on Warm Called Crucial in Iran Nuclear Delay". *The New York Times*. 15 January 2011.

Carr, John. "Online Crimes against Children". *F3 Freedom from Fear* 7 (2010). Last accessed 12 October 2011. <http://www.freedomfromfearmagazine.org/index.php?option=com_content&view=article&id=308:online-crimes-against-children-&catid=50:issue-7&Itemid=187>

Chiesa, Raoul. *Profiling Hackers: The Science of Criminal Profiling as Applied to the World of Hacking*. UNICRI: Turin, 2008.

Chinkin, C. M. "The Challenge of Soft Law: Development and Change in International Law." *The International and Comparative Law Quarterly* 38.4 (1989): 850-66.

Clarke, Richard A. and Robert Knake. *Cyber War : The Next Threat to National Security and What To Do About It*. Ecco, April 2010.

Deibert, Ronald. "Ronald Deibert: Tracking the emerging arms race in cyberspace". *Bulletin of the Atomic Scientists 67.1 (January/February 2011). Last accessed 12 October 2011.* <http://bos.sagepub.com/content/67/1/1.abstract>

Eriksson, Johan and Giampiero Giacomello. "The Information Revolution, Security, and International Relations: (IR)relevant Theory?" *International Political Science Review* 27.3 (2006): 221-244.

Finnemore, Martha, and Kathryn Sikkink. "International Norm Dynamics and Political Change." *International Organization* 52.4 (1998): 894-905.

Ford, Christopher A. “The Trouble with Cyber Arms Control”. *The New Atlantis – A Journal of Technology & Society*. (Fall 2010): 52-67.

Geers, Kenneth. “Cyber Weapons Convention”. *Computer Law and Security Review* 23 (2010): 547-551

Gorman, Siobhan. “U.S. Backs Talks on Cyber Warfare”. *The Wall Street Journal* (4 June 2010). Last accessed 12 October 2011. <http://online.wsj.com/article/SB10001424052748703340904575284964215965730.html>

Hall and Taylor. “Political Science and the Three New Institutionalisms”. *Political Studies* XLIV (1996): 955-956

Hillgenberg, Hartmut. “A Fresh Look at Soft Law”. *European Journal of International Law* 10.3 (1999): 499-515.

Kingdon, John W. *Agenda, Alternatives, and Public Policies*. New York: Longman, 2003.

Komov, Sergei, Sergei Korotkov and Igor Dylevski. “Military aspects of ensuring internaitonal information security in the context of elaborating universally acknowledged principles of internaitonal law”. *Disarmament Forum* 3 (2007) Last accessed 12 October 2011. <http://www.unidir.org/pdf/articles/pdf-art2645.pdf>

Krasner, Stephen. *International Regimes.* Ithaca, NY: Cornell University Press, 1983: 2

Lakoff, George. *Thinking Points: Communicating our American Values and Visions*. Farrar, Straus, and Giroux: 2006.

Lessig, Lawrence. “The regulation of social meaning”. *The University of Chicago Law Review* 62.3 (1995): 944-1045.

March, James G., and Johan P. Olsen. "The Institutional Dynamics of International Political Orders." *International Organization* 52.4 (1998): 943-69.

Markoff, John and Andrew E. Kramer. “In Shift, U.S. Talks to Russia on Internet Security”. *The New York Times*. 13 December 2009.

Markoff, John. “Step Taken to End Impasse Over Cybersecurity Talks”. *The New York Times*. 16 July 2010.

McCarthy, Kieren. “Global Internet governance fight looms”. *.nxt blog* (22 September 2011). Last accessed 12 October 2011. <http://news.dot-nxt.com/2011/09/22/internet-governance-fight-looms>

Nakashima, Ellen. “15 nations agree to start working together to reduce cyberwarfare threat”. *The Washington Post*. 17 July 2010.

Nazli, Choucri. “Introduction: CyberPolitics in International Relations” *International Political Science Review* 21.3 (2000): 243-263.

Nye Jr, Joseph S. “Nuclear Lessons for Cyber Security?” *Strategic Studies Quarterly* (forthcoming 2011)

Nye Jr, Joseph S. “Cyberpower”. *Paper*. Cambridge, Mass.: Harvard Belfer Center for Science and International Affairs, May 2010.

Pradesh, Andhra. “ITU mullying ‘cyber treaty’ to curb cyber crime” *The Hindu* (25 May 2011). Last accessed 12 October 2011. <http://www.hindu.com/2010/05/25/stories/2010052562310800.htm>

Russian Federation. *Convention on International Information Security (Concept)*. Ekaterinburg, Russia: International Meeting of High-Ranking Officials Responsible for Security Matters, 21-22 September 2011.

Schwartau, Winn. “Testimony before Congress” (27 June 1991). Last accessed 12 October 2011. <http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA344848>

Segal, Adam. “China and Information vs. Cyber Security” Council on Foreign Relations blog (15 September 2011). Last accessed 3 October 2011. <http://blogs.cfr.org/asia/2011/09/15/china-and-information-vs-cybersecurity/>

Singer, Peter W. “The Wrong War: The Insistence on Applying Cold War Metaphors to Cybersecurity is Misplaced and Counterproductive”. Brookings Government Executive. Last accessed 12 October 2011. < http://www.brookings.edu/articles/2011/0815_cybersecurity_singer_shachtman.aspx>

Streltsov, A.A. “International information security: description and legal aspects”. *Disarmament Forum* 3 (2007) Last accessed 12 October 2011. <http://www.unidir.org/pdf/articles/pdf-art2642.pdf>

The Hindu Business Line. “Cyber war: Take no-first-attack vow, ITU tells nations” (24 May 2010). Last accessed 12 October 2011. <http://www.thehindubusinessline.in/bline/2010/05/25/stories/2010052552450700.htm>

Toure, Hamadoun I. “Cyberspace and the Threat of Cyberwar”, in *The Quest for Cyber Peace.* International Telecommunication Union and World Federation of Scientists, January 2011.

Toure, Hamadoun I. “ITU’s Global Cybersecurity Agenda”, in *The Quest for Cyber Peace.* International Telecommunication Union and World Federation of Scientists, January 2011.

Toure, Hamadoun I. “The International Response to Cyberwar”, in *The Quest for Cyber Peace.* International Telecommunication Union and World Federation of Scientists, January 2011.

United Nations. Counter-Terrorism Implementation Task Force. “CTITF Working Group Compendium – Countering the Use of the Internet for Terrorist Purposes – Legal and Technical Aspects”. *CTITF Publication Series.* New York: United Nations, May 2011.

United Nations. Counter-Terrorism Implementation Task Force. “Main Page”. Last accessed 3 August 2010. <www.un.org/terrorism/cttaskforce.shtml>

United Nations. Counter-Terrorism Implementation Task Force. *Report of the Working Group on Countering the Use of the Internet for Terrorist Purposes*. New York: United Nations, February 2009.

United Nations. Counter-Terrorism Implementation Task Force. “Working Groups”. Last accessed 3 August 2010. < https://www.un.org/terrorism/workinggroups.shtml>

United Nations. Counter-Terrorism Implementation Task Force. "Working Group on Countering the Use of the Internet for Terrorist Purposes". Last accessed 12 October 2011. <http://www.un.org/terrorism/internet>

United Nations. Economic and Social Council. *2010 ECOSOC General segment briefing on 'Cyber security: emerging threats and challenges' Friday, 16 July, 3:00-4:30 p.m. Background Note.* Last accessed 12 October 2011. <https://www.un.org/en/ecosoc/julyhls/pdf10/gs_briefing_background_note.pdf>

United Nations. Economic and Social Council. *2010 ECOSOC General segment briefing on 'Cyber security: emerging threats and challenges' Friday, 16 July, 3:00-4:30 p.m. Statements.* Last accessed 12 October 2011. <https://www.un.org/en/ecosoc/julyhls/pdf10/cyber_security_statement.pdf>

United Nations. Economic and Social Council. *Commission on Crime Prevention and Criminal Justice: Report of the Secretary-General – International cooperation in the prevention, investigation, prosecution and punishment of economic fraud and identity-related crime*. E/CN.15/2009/2. New York: United Nations, 3 February 2009.

United Nations. Economic and Social Council. *Commission on Crime Prevention and Criminal Justice: Report of the Secretary-General – Results of the second meeting of the Intergovernmental Expert Group to Prepare a Study on Fraud and the Criminal Misuse and Falsification of Identity*. E/CN.15/2007/8*. New York: United Nations, 2 April 2007.

United Nations. Economic and Social Council. *Commission on Crime Prevention and Criminal Justice – Report on the twentieth session*. E/2011/30*. New York: United Nations, 2011.

United Nations. Economic and Social Council. *Commission on Crime Prevention and Criminal Justice – Report on the nineteenth session*. E/2010/30. New York: United Nations, 2010.

United Nations. Economic and Social Council. *Commission on Crime Prevention and Criminal Justice – Report on the third session*. E/19940/31. New York: United Nations, 1994.

United Nations. Economic and Social Council. *Commission on Narcotic Drugs – Report on the fiftieth session: Resolution 50/11*. E/2007/28/Rev.1. New York: United Nations, 2007.

United Nations. Economic and Social Council. *Commission on Narcotic Drugs – Report on the forty-eighth session: Resolution 48/5*. E/2005/28. New York: United Nations, 30 March 2005.

United Nations. Economic and Social Council. *Commission on Narcotic Drugs – Report on the forty-seventh session*. E/2004/28. New York: United Nations, 2004.

United Nations. Economic and Social Council. *Commission on Narcotic Drugs – Report on the forty-third session: Resolution 43/8*. E/2000/28. New York: United Nations, 2000.

United Nations. Economic and Social Council. *Commission on Narcotic Drugs – Report on the forty-second session*. E/1999/28/Rev.1. New York: United Nations, 1999.

United Nations. Economic and Social Council. *Resolution 2010/18 – Twelfth United Nations Congress on Crime Prevention and Criminal Justice*. E/2010/18. New York: United Nations, 22 July 2010.

United Nations. Economic and Social Council. *Resolution 2009/22 – International cooperation in the prevention, investigation, prosecution and punishment of economic fraud and identity related-crime*. E/2010/18. New York: United Nations, 30 July 2009.

United Nations. Economic and Social Council. *Resolution 2004/26 – International cooperation in the prevention, prosecution and punishment of fraud, the criminal misuse and falsification of identity and related crimes*. E/2004/26. New York: United Nations, 21 July 2004.

United Nations. General Assembly. *First Committee draft resolution - Developments in the field of information and telecommunications in the context of international security*. A/C.1/61/L.35. New York: United Nations, 11 October 2006.

United Nations. General Assembly. *Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General*. A/66/359. New York: United Nations, 14 September 2011.

United Nations. General Assembly. *Note by the Secretary-General 65/201 - Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*. A/65/201. New York: United Nations, 30 July 2010.

United Nations. General Assembly. *Report of the First Committee 65/405 - Developments in the field of information and telecommunications in the context of international security*. A/65/405. New York: United Nations, 9 November 2010.

United Nations. General Assembly. *Report of the First Committee 61/389 - Developments in the field of information and telecommunications in the context of international security*. A/61/389. New York: United Nations, 9 November 2006.

United Nations. General Assembly. *Report of the First Committee 60/452 - Developments in the field of information and telecommunications in the context of international security*. A/60/452. New York: United Nations, 16 November 2005.

United Nations. General Assembly. *Report of the Second Committee 64/422/Add. 3 – Globalization and Interdependence: science and technology for development*. A/64/422/Add.3. New York: United Nations, 15 December 2009.

United Nations. General Assembly. *Report of the Second Committee 58/481/Add. 2 - Macroeconomic policy questions: science and technology for development*. A/58/481/Add.2. New York: United Nations, 15 December 2003.

United Nations. General Assembly. *Report of the Second Committee 57/529/Add. 3 - Macroeconomic policy questions: science and technology for development*. A/57/529/Add.3. New York: United Nations, 12 December 2002.

United Nations. General Assembly. *Report of the Secretary-General 60/202 - Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*. A/60/202. New York: United Nations, 5 August 2005.

United Nations. General Assembly. *Report of the Third Committee 65/457 - Crime prevention and criminal justice*. A/65/457. New York: United Nations, 6 December 2010.

United Nations. General Assembly. *Report of the Third Committee 64/440 - Crime prevention and criminal justice*. A/64/440. New York: United Nations, 1 December 2009.

United Nations. General Assembly. *Report of the Third Committee 63/431 - Crime prevention and criminal justice*. A/63/431. New York: United Nations, 4 December 2008.

United Nations. General Assembly. *Report of the Third Committee 56/574 - Crime prevention and criminal justice.* A/56/574. New York: United Nations, 7 December 2001.

United Nations. General Assembly. *Report of the Third Committee/55/593 - Crime prevention and criminal justice*. A/55/593. New York: United Nations, 16 November 2000.

United Nations. General Assembly. *Report of the Twelfth United Nations Congress on Crime Prevention and Criminal Justice*. A/CONF.213/18. Salvador, Brazil: United Nations, 18 May 2010.

United Nations. General Assembly. *Resolution 65/232 - Strengthening the United Nations crime prevention and criminal justice programme, in particular its technical cooperation capacity*. A/RES/65/232. New York: United Nations, 23 March 2011.

United Nations. General Assembly. *Resolution 65/230 - Twelfth United Nations Congress on Crime Prevention and Criminal Justice*. A/RES/65/230. New York: United Nations, 1 April 2011.

United Nations. General Assembly. *Resolution 64/211 - Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures.* A/RES/64/211. New York: United Nations, 17 March 2011.

United Nations. General Assembly. *Resolution 63/193 – Preparations for the Twelfth United Nations Congress on Crime Prevention and Criminal Justice*. A/RES/63/193. New York: United Nations, 24 February 2009.

United Nations. General Assembly. *Resolution 60/288 – The United Nations Global Counter-Terrorism Strategy.* A/RES/60/288. New York: United Nations, 20 September 2006.

United Nations. General Assembly. *Resolution 57/239 - Creation of a global culture of cybersecurity*. A/RES/57/239. New York: United Nations, 31 January 2003.

United Nations. General Assembly. *Resolution 56/121 - Combating the criminal misuse of information technologies*. A/RES/56/121. New York: United Nations, 23 January 2002.

United Nations. General Assembly. *Resolution 55/63 - Combating the criminal misuse of information technologies*. A/RES/55/63. New York: United Nations, 22 January 2001.

United Nations. General Assembly. *Resolution 53/70 - Developments in the field of information and telecommunications in the context of international security*. A/RES/53/70. New York: United Nations, 4 January 1999.

United Nations. General Assembly. *Resolution S-20/4 - Measures to enhance international cooperation to counter the world drug problem*. A/RES/S-20/4*. New York: United Nations, 21 October 1998.

United Nations. Institute for Disarmament Research. *Agenda – Information & Communication Technologies and International Security – 24-25 April 2008*. Last accessed 12 October 2011. <http://www.unidir.org/pdf/activites/pdf-act371.pdf>

United Nations. Institute for Disarmament Research. "Conference – Developments in the field of information and telecommunication in the context of international security". Last accessed 12 October 2011. < http://www.unidir.org/bdd/fiche-activite.php?ref_activite=81>

United Nations. Institute for Disarmament Research. "Conference – Information and Communication Technologies and International Security". Last accessed 12 October 2011. <http://www.unidir.org/bdd/fiche-activite.php?ref_activite=371>

United Nations. Institute for Disarmament Research. "ICTs and International Security" *Disarmament Forum* 3 (2007). Last accessed 12 October 2011. <http://www.unidir.org/bdd/fiche-periodique.php?ref_periodique=1020-7287-2007-3-en#contents>

United Nations. Institute for Disarmament Research. "Research Project – Group of Governmental Experts on the Issue of Information Security (2009-2010)". Last accessed 12 October 2011. <http://www.unidir.org/bdd/fiche-activite.php?ref_activite=483>

United Nations. Institute for Disarmament Research. "Research Project – Perspectives on Cyber War: Legal Frameworks and Transparency and Confidence Building". Last accessed 12 October 2011. <http://www.unidir.org/bdd/fiche-activite.php?ref_activite=583>

United Nations. Institute for Disarmament Research. *Summary - Developments in the field of information and telecommunication in the context of international security*. Last accessed 12 October 2011. <http://www.unidir.org/pdf/activites/pdf2-act81.pdf>

United Nations. International Telecommunication Union. "Child Online Protection". Last accessed 12 October 2011. <http://www.itu.int/osg/csd/cyber-security/gca/cop/meetings/june-tokyo/bios/index.html>

United Nations. International Telecommunication Union. *Cybersecurity for all – Global Cybersecurity Agenda: A Framework for International Cooperation*. Geneva: United Nations, March 2010.

United Nations. International Telecommunication Union. *ITU Global Cybersecurity Agenda: High Level Experts Group – Global Strategic Report*. Geneva: United Nations, 2008.

United Nations. International Telecommunication Union. "Overview of cybersecurity – Recommendation ITU-T X.1205". *Series X: Data Networks, Open System Communications and Security" – Telecommunication security*. Geneva: United Nations, April 2008.

United Nations. International Telecommunication Union. “PowerPoint Presentation on Global Cybersecurity Agenda to Open-ended Intergovernmental Expert Group on Cybercrime – Vienna, 17-21 January 2011”. Last accessed 8 October 2011. <https://www.unodc.org/documents/treaties/organized_crime/EGM_cybercrime_2011/Presentations/ITU_Cyber crime_ EGMJan2011.pdf>

United Nations. Internet Governance Forum. “About the Internet Governance Forum”. Last accessed 12 October 2011. <http://www.intgovforum.org/cms/aboutigf>

United Nations. Internet Governance Forum. “Past Staff Members”. Last accessed 12 October 2011. <http://www.intgovforum.org/cms/component/content/article/762-past-staff-members>

United Nations. Interregional Crime and Justice Research Institute. “Cybercrimes - UNICRI's Initiatives”. Last accessed 12 October 2011. <http://www.unicri.it/emerging_crimes/cybercrime/initiatives/>

United Nations. Office on Drugs and Crime. “Law enforcement officers trained to tackle cybercrime”. (19 June 2009) Last accessed 12 October 2011. <https://www.unodc.org/unodc/en/frontpage/2009/June/law-enforcement-officers-trained-in-tackling-cybercrime.html>

United Nations. Office on Drugs and Crime. “Open-ended intergovernmental expert group to conduct a comprehensive study of the problem of cybercrime - Vienna, 17-21 January 2011”. Last accessed 12 October 2011. <https://www.unodc.org/unodc/en/expert-group-to-conduct-study-cybercrime-jan-2011.html>

United Nations. Office on Drugs and Crime. “Secretariat to the Governing Bodies Section”. Last accessed 12 October 2011. < https://www.unodc.org/unodc/en/commissions/secretariat2.html?ref=menuside>

United Nations. Security Council. Counter-Terrorism Committee. “About Us”. Last accessed 12 October 2011. <http://www.un.org/en/sc/ctc/aboutus.html>

United Nations. Unicef. “Child protection from violence, exploitation and abuse”. Last accessed 12 October 2011. <http://www.unicef.org/protection/57929_57985.html>

United Nations. World Summit on the Information Society. *Report of the Tunis phase of the World Summit on the Information Society, Tunis, Kram Palexpo, 16-18 November 2005*. WSIS-05/TUNIS/DOC/9Rev.1)-E. Tunis: United Nations, 15 February 2006.

Wegener, Henning. “Cyber Peace”, in *The Quest for Cyber Peace.* International Telecommunication Union and World Federation of Scientists, January 2011.

Wegener, Henning. “Harnessing the perils in cyberspace: who is in charge?” *Disarmament Forum* 3 (2007) Last accessed 12 October 2011. <http://www.unidir.org/pdf/articles/pdf-art2645.pdf>

Wikipedia. “History of the Internet”. Last accessed 12 October 2011. <https://secure.wikimedia.org/wikipedia/en/wiki/History_of_the_Internet>

World Federation of Scientists. "The Erice Statement". Last accessed 12 October 2011. <http://www.federationofscientists.org/WfsErice.asp>

World Federation of Scientists. *Toward a Universal Order of Cyberspace: Managing Threats from Cybercrime to Cyberwar.* WSIS-03/GENEVA/CONTR/6. World Summit on the Information Society, 2003.

Wu, Tim and Jack Goldsmith. *Who Controls the Internet – Illusions of a Borderless World*. Oxford: Oxford University Press, 2008.

Interviewees

Bosco, Francesca. Project Officer. United Nations Interregional Crime & Justice Research Institute. Email correspondence with author. September 2011.

Chiesa, Raoul. Senior Advisor, Strategic Alliances & Cybercrime Issues. United Nations Interregional Crime & Justice Research Institute. Email correspondence with author and interview with author. Turin, Italy. August 6, 2010.

Neutze, Jan. Programme Officer. Counter-Terrorism Implementation Task Force. United Nations. Phone interview with author. August 30, 2010.

Ntoko, Alexander. Head of Corporate Strategy Division. International Telecommunications Union. Email correspondence with author and interview with author. Geneva, Switzerland. August 3, 2010.

Some officials preferred to remain anonymous.

General Assembly Resolution 57/239

Creation of a global culture of cybersecurity

The General Assembly, […] *Takes note* of the elements annexed to the present resolution, with a view to creating a global culture of cybersecurity […]

78th plenary meeting
20 December 2002

Annex

Elements for creating a global culture of cybersecurity

Rapid advances in information technology have changed the way Governments, businesses, other organizations and individual users who develop, own, provide, manage, service and use information systems and networks ("participants") must approach cybersecurity. A global culture of cybersecurity will require that all participants address the following nine complementary elements:

(*a*) *Awareness.* Participants should be aware of the need for security of information systems and networks and what they can do to enhance security;

(*b*) *Responsibility*. Participants are responsible for the security of information systems and networks in a manner appropriate to their individual roles. They should review their own policies, practices, measures and procedures regularly, and should assess whether they are appropriate to their environment;

(*c*) *Response*. Participants should act in a timely and cooperative manner to prevent, detect and respond to security incidents. They should share information about threats and vulnerabilities, as appropriate, and implement procedures for rapid and effective cooperation to prevent, detect and respond to security incidents. This may involve cross-border information-sharing and cooperation;

(*d*) *Ethics*. Given the pervasiveness of information systems and networks in modern societies, participants need to respect the legitimate interests of others and recognize that their action or inaction may harm others;

(*e*) *Democracy*. Security should be implemented in a manner consistent with the values recognized by democratic societies, including the freedom to exchange thoughts and ideas, the free flow of information, the confidentiality of information and communication, the appropriate protection of personal information, openness and transparency;

(*f*) *Risk assessment*. All participants should conduct periodic risk assessments that identify threats and vulnerabilities; are sufficiently broad-based to encompass key internal and external factors, such as technology, physical and human factors, policies and third-party services with security implications; allow determination of the acceptable level of risk; and assist in the selection of appropriate controls to manage the risk of potential harm to

information systems and networks in the light of the nature and importance of the information to be protected;

(*g*) *Security design and implementation*. Participants should incorporate security as an essential element in the planning and design, operation and use of information systems and networks;

(*h*) *Security management*. Participants should adopt a comprehensive approach to security management based on risk assessment that is dynamic, encompassing all levels of participants' activities and all aspects of their operations;

(*i*) *Reassessment*. Participants should review and reassess the security of information systems and networks and should make appropriate modifications to security policies, practices, measures and procedures that include addressing new and changing threats and vulnerabilities.

General Assembly Resolution 58/199

Creation of a global culture of cybersecurity and the protection of critical information infrastructures

The General Assembly, […] *Takes note* of the elements set out in the annex to the present resolution for protecting critical information infrastructures […]

78th plenary meeting
23 December 2003

Annex

Elements for protecting critical information infrastructures

1. Have emergency warning networks regarding cyber-vulnerabilities, threats and incidents.

2. Raise awareness to facilitate stakeholders' understanding of the nature and extent of their critical information infrastructures and the role each must play in protecting them.

3. Examine infrastructures and identify interdependencies among them, thereby enhancing the protection of such infrastructures.

4. Promote partnerships among stakeholders, both public and private, to share and analyse critical infrastructure information in order to prevent, investigate and respond to damage to or attacks on such infrastructures.

5. Create and maintain crisis communication networks and test them to ensure that they will remain secure and stable in emergency situations.

6. Ensure that data availability policies take into account the need to protect critical information infrastructures.

7. Facilitate the tracing of attacks on critical information infrastructures and, where appropriate, the disclosure of tracing information to other States.

8. Conduct training and exercises to enhance response capabilities and to test continuity and contingency plans in the event of an information infrastructure attack, and encourage stakeholders to engage in similar activities.

9. Have adequate substantive and procedural laws and trained personnel to enable States to investigate and prosecute attacks on critical information infrastructures and to coordinate such investigations with other States, as appropriate.

10. Engage in international cooperation, when appropriate, to secure critical information infrastructures, including by developing and coordinating emergency warning systems, sharing and analysing information regarding vulnerabilities, threats and incidents and coordinating investigations of attacks on such infrastructures in accordance with domestic laws.

11. Promote national and international research and development and encourage the application of security technologies that meet international standards.

General Assembly Resolution 64/211

Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures

The General Assembly, […] *Invites* Member States to use, if and when they deem appropriate, the annexed voluntary self-assessment tool for national efforts to protect critical information infrastructures in order to assist in assessing their efforts in this regard to strengthen their cybersecurity, so as to highlight areas for further action, with the goal of increasing the global culture of cybersecurity […]

66th plenary meeting
21 December 2009

Annex

Voluntary self-assessment tool for national efforts to protect critical information infrastructures[175]

Taking stock of cybersecurity needs and strategies

1. Assess the role of information and communications technologies in your national economy, national security, critical infrastructures (such as transportation, water and food supplies, public health, energy, finance, emergency services) and civil society.

2. Determine the cybersecurity and critical information infrastructure protection risks to your economy, national security, critical infrastructures and civil society that must be managed.

3. Understand the vulnerabilities of the networks in use, the relative levels of threat faced by each sector at present and the current management plan; note how changes in the economic environment, national security priorities and civil society needs affect these calculations.

4. Determine the goals of the national cybersecurity and critical information infrastructure protection strategy; describe its goals, the current level of implementation, measures that exist to gauge its progress, its relation to other national policy objectives and how such a strategy fits within regional and international initiatives.

Stakeholder roles and responsibilities

5. Determine key stakeholders with a role in cybersecurity and critical information infrastructure protection and describe the role of each in the development of relevant policies and operations, including:

- National Government ministries or agencies, noting primary points of contact and responsibilities of each;

[175] This is a voluntary tool that may be used by Member States, in part or in its entirety, if and when they deem appropriate, in order to assist in their efforts to protect their critical information infrastructures and strengthen their cybersecurity.

- Other government (local and regional) participants;
- Non-governmental actors, including industry, civil society and academia;
- Individual citizens, noting whether average users of the Internet have access to basic training in avoiding threats online and whether there is a national awareness-raising campaign regarding cybersecurity.

Policy processes and participation

6. Identify formal and informal venues that currently exist for Government-industry collaboration in the development of cybersecurity and critical information infrastructure protection policy and operations; determine participants, role(s) and objectives, methods for obtaining and addressing input, and adequacy in achieving relevant cybersecurity and critical information infrastructure protection goals.

7. Identify other forums or structures that may be needed to integrate the government and non-government perspectives and knowledge necessary to realize national cybersecurity and critical information infrastructure protection goals.

Public-private cooperation

8. Collect all actions taken and plans to develop collaboration between government and the private sector, including any arrangements for information-sharing and incident management.

9. Collect all current and planned initiatives to promote shared interests and address common challenges among both critical infrastructure participants and private-sector actors mutually dependent on the same interconnected critical infrastructure.

Incident management and recovery

10. Identify the Government agency that serves as the coordinator for incident management, including capability for watch, warning, response and recovery functions; the cooperating Government agencies; non-governmental cooperating participants, including industry and other partners; and any arrangements in place for cooperation and trusted information-sharing.

11. Separately, identify national-level computer incident response capacity, including any computer incident response team with national responsibilities and its roles and responsibilities, including existing tools and procedures for the protection of Government computer networks, and existing tools and procedures for the dissemination of incident-management information.

12. Identify networks and processes of international cooperation that may enhance incident response and contingency planning, identifying partners and arrangements for bilateral and multilateral cooperation, where appropriate.

Legal frameworks

13. Review and update legal authorities (including those related to cybercrime, privacy, data protection, commercial law, digital signatures and encryption) that may be outdated or obsolete as a result of the rapid uptake of and dependence upon new information and communications technologies, and use regional and international conventions, arrangements and precedents in these reviews. Ascertain whether your country has developed necessary

legislation for the investigation and prosecution of cybercrime, noting existing frameworks, for example, General Assembly resolutions 55/63 and 56/121 on combating the criminal misuse of information technologies, and regional initiatives, including the Council of Europe Convention on Cybercrime.

14. Determine the current status of national cybercrime authorities and procedures, including legal authorities and national cybercrime units, and the level of understanding among prosecutors, judges and legislators of cybercrime issues.

15. Assess the adequacy of current legal codes and authorities in addressing the current and future challenges of cybercrime, and of cyberspace more generally.

16. Examine national participation in international efforts to combat cybercrime, such as the round-the-clock Cybercrime Point of Contact Network.

17. Determine the requirements for national law enforcement agencies to cooperate with international counterparts to investigate transnational cybercrime in those instances in which infrastructure is situated or perpetrators reside in national territory, but victims reside elsewhere.

Developing a global culture of cybersecurity

18. Summarize actions taken and plans to develop a national culture of cybersecurity referred to in General Assembly resolutions 57/239 and 58/199, including implementation of a cybersecurity plan for Government-operated systems, national awareness-raising programmes, outreach programmes to, among others, children and individual users, and national cybersecurity and critical information infrastructure protection training requirements.

Annex to the letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General (A/66/359)

International code of conduct for information security

The General Assembly,

Recalling its resolutions on the role of science and technology in the context of international security, in which, inter alia, it recognized that scientific and technological developments could have both civilian and military applications and that progress in science and technology for civilian applications needed to be maintained and encouraged,

Noting that considerable progress has been achieved in developing and applying the latest information technologies and means of telecommunication,

Recognizing the need to prevent the potential use of information and communication technologies for purposes that are inconsistent with the objectives of maintaining international stability and security and may adversely affect the integrity of the infrastructure within States, to the detriment of their security,

Underlining the need for enhanced coordination and cooperation among States in combating the criminal misuse of information technologies and, in that context, stressing the role that can be played by the United Nations and other international and regional organizations,

Highlighting the importance of the security, continuity and stability of the Internet and the need to protect the Internet and other information and communications technology networks from threats and vulnerabilities, and reaffirming the need for a common understanding of the issues of Internet security and for further cooperation at the national and international levels,

Reaffirming that policy authority for Internet-related public issues is the sovereign right of States, which have rights and responsibilities for international Internet-related public policy issues,

Recognizing that confidence and security in the use of information and communications technologies are among the main pillars of the information society and that a robust global culture of cybersecurity needs to be encouraged, promoted, developed and vigorously implemented, pursuant to General Assembly resolution 64/211 of 21 December 2009, entitled "Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures",

Stressing the need for enhanced efforts to close the digital divide by facilitating the transfer of information technology and capacity-building to developing countries in the areas of cybersecurity best practices and training, pursuant to resolution 64/211,

Adopts the international code of conduct for information security as follows:

Purpose and scope

The purpose of the present code is to identify the rights and responsibilities of States in information space, promote their constructive and responsible behaviours and enhance their cooperation in addressing the common threats and challenges in information space, so as to ensure that information and communications technologies, including networks, are to be solely used to benefit social and economic development and people's well-being, with the objective of maintaining international stability and security.

Adherence to the code is voluntary and open to all States.

Code of conduct

Each State voluntarily subscribing to the code pledges:

(a) To comply with the Charter of the United Nations and universally recognized norms governing international relations that enshrine, inter alia, respect for the sovereignty, territorial integrity and political independence of all States, respect for human rights and fundamental freedoms and respect for the diversity of history, culture and social systems of all countries;

(b) Not to use information and communications technologies, including networks, to carry out hostile activities or acts of aggression, pose threats to international peace and security or proliferate information weapons or related technologies;

(c) To cooperate in combating criminal and terrorist activities that use information and communications technologies, including networks, and in curbing the dissemination of information that incites terrorism, secessionism or extremism or that undermines other countries' political, economic and social stability, as well as their spiritual and cultural environment;

(d) To endeavour to ensure the supply chain security of information and communications technology products and services, in order to prevent other States from using their resources, critical infrastructures, core technologies and other advantages to undermine the right of the countries that have accepted the code of conduct, to gain independent control of information and communications technologies or to threaten the political, economic and social security of other countries;

(e) To reaffirm all the rights and responsibilities of States to protect, in accordance with relevant laws and regulations, their information space and critical information infrastructure from threats, disturbance, attack and sabotage;

(f) To fully respect rights and freedom in information space, including rights and freedom to search for, acquire and disseminate information on the premise of complying with relevant national laws and regulations;

(g) To promote the establishment of a multilateral, transparent and democratic international Internet management system to ensure an equitable distribution of resources, facilitate access for all and ensure a stable and secure functioning of the Internet;

(h) To lead all elements of society, including its information and communication partnerships with the private sector, to understand their roles and responsibilities with regard to information security, in order to facilitate the creation of a culture of information security and the protection of critical information infrastructures;

(i) To assist developing countries in their efforts to enhance capacity-building on information security and to close the digital divide;

(j) To bolster bilateral, regional and international cooperation, promote the important role of the United Nations in formulating international norms, peaceful settlements of international disputes and improvements in international cooperation in the field of information security, and enhance coordination among relevant international organizations;

(k) To settle any dispute resulting from the application of the code through peaceful means and to refrain from the threat or use of force.

Belfer Center for Science and International Affairs
Harvard Kennedy School
79 JFK Street
Cambridge, MA 02138
Fax: (617) 495-8963
Email: belfer_center@harvard.edu
Website: http://belfercenter.org