# Expanding the Mandate of the ITU?

Catherine Lotrionte
Georgetown University
Washington D.C., USA
lotrionc@georgetown.edu

**Abstract—The disagreements among states that occurred in December 2012 at the World Conference on International Telecommunications in Dubai about appropriate revisions to the International Telecommunications Regulations highlighted the controversy over what the appropriate role of the ITU ought to be in the age of the Internet. Some have argued that the ITU should remain focused exclusively on technical and economic issues. Recently, others have advocated for an expanded role for the ITU, recommending that the ITU take on security issues in an effort to constrain espionage and cyber conflict. This article outlines why the ITU is not the appropriate organization to regulate such matters of "high politics," demonstrating under international law that there are existing competent institutions to manage the challenges related to issues of intervention, use of force and aggression in the cyber domain.**

## I. Introduction

In December 2012, the International Telecommunication Union (ITU) convened the World Conference on International Telecommunications (WCIT-12) to amend the International Telecommunication Regulations (ITRs), an ITU treaty adopted in 1988 to foster more effective cooperation on provision of international telecommunication services (i.e., telegraph and telephone).[1] The WCIT-12 negotiations, however, failed to reach consensus, particularly about whether the revised ITRs should apply to the Internet and its governance, giving the ITU an expanded role in the management of the Internet. Although the Secretary General of the ITU repeatedly stated that the WCIT-12 would not be about Internet governance, proposals by ITU members included changes to the ITRs focused on the Internet and how it is governed.[2] Ultimately, 89 states signed the revised ITRs and 55 states (including the US and members of the EU) did not sign the revised treaty.[3] This article does not address the debate over the appropriate relationship between the ITU and the Internet technical community. Rather, it discusses the challenges of international organizations in international relations, highlighting important shortcoming. It then explains why issues of cyberespionage and cyberwarfare, in particular, should not be part of the ITU mandate but left to other institutions to manage.

## II. Run Up to WCIT-12

### A. *Member States' Positions*

The controversial proposed revisions of the ITRs should have been no surprise for those following the signals from the ITU and its member states. Since the emergence of the Internet, the ITU has been in search for a new mission, one that exceeds the original intent of its members. Some member states have been seeking more state imposed limitations and international law for the Internet under the auspices of the ITU. In 2011, Russian President Vladimir Putin declared the importance of "establishing international control over the Internet using the monitoring and supervisory capabilities of the International Telecommunication Union."[4] Not surprisingly, at WCIT-12 the Russian proposals for the ITRs, supported by Arab states, included calls for more control over behavior on the Internet. Others states, fearing that they had been at a disadvantage to the US' ability to use the Internet for military and political purposes followed suit in these attempts to move the ITU state-centric regime into the sphere of governance of the Internet.

In December 2003, China proposed creating an international Internet organization and adopting an Internet treaty.[5] In 2011, Russia, China, Tajikistan and Uzbekistan submitted a proposal for an *International Code of Conduct for Information Security*[6] at the UN General Assembly. This proposal called for international agreement to censor certain information on the Internet deemed threatening to a state's

[1] International Telecommunication Union, Review of the International Telecommunication Regulations, ITU Admin. Council Res. 146 (2006), http://www.itu.int/ITU-T/itr-eg/files/resolution146.pdf. The ITU convenes world conferences on international telecommunications specifically to revise the ITRs under the ITU Convention. ITU Const., Article 25(1). Revisions of the ITRs become binding on ITU member states when they consent to be bound by the revisions. ITU Const., Article 54.

[2] ITU, *Proposals Received from ITU Member States for the Work of the Conference*, 99 Doc. WCIT12/DT/1-E (2012), http://www.soumu.go.jp/main_content/000188223.pdf.

[3] ITU, *WCIT 2012: Signatories of the Final Acts*, http://www.itu.int/osg/wcit-12/highlights/signatories.html.

[4] Transcript, *Prime Minister Vladmir Putin meets with Secretary General of the International Telecommunication Union Hamadoun Toure*, Website of the Government of the Russian Federation (June 15, 2011).

[5] Wolfgang Kleinwachter, *The History of Internet Governance, Internet Governance* (Oct. 20, 2009), http://www.intgov.net/papers/35.

[6] UNGA Res. A/66/359, "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." September 14, 2011; http://www.citizenlab.org/cybernorms/letter.pdf.

political stability. Having failed at earlier attempts to gain international support to regulate the Internet, WCIT-12 became an opportunity for states seeking to achieve their objectives regardless of the inadequacies of the forum, the means and the international organization of choice.

### B. *The ITU's Expansive Agenda*

Regardless of how often the ITU Secretary General, Hamadoun Toure, publicly and emphatically stated that WCIT-12 would not be about the Internet, his words quickly lost legitimacy as the conference unfolded and Internet regulation was a topic for discussion. Previously Toure had warned that if the ITU did not get involved with the Internet it would collapse, arguing that without changes to ITR provisions, "we risk the collapse of ICT networks which underpin all communications technologies."[7]

In support of the ITR revisions, the ITU, in its own document entitled "Security in the Use of ICTs," identified different "global challenges" related to the security of the Internet, providing a "cyberattack timeline" that includes a description of the Google incident in China as "Google email system hacked, attack suspected to originate from China."[8] While ITU officials and staff have no voting authority within the treaty-making process, their role in framing the issues, setting the agenda, managing procedural items and establishing the "tone" for dialogue at the conferences imbues them with a level of influence on the direction and substance of the issues.

The deliberations over contested proposals at WCIT-12 reflected the buildup that preceded the conference and states' strategic and political agendas with regard to the Internet. Revelations subsequent to WCIT-12's conclusion –including leaks about the US' surveillance programs—have only deepened the sense that power politics in cyberspace has entered a new phase where states will seek to enhance their power and influence through the ITU to address security threats they perceive through the Internet. One of the more significant effects from the recent spying revelations may ultimately be the leverage they provided for those calling for more regulation of the Internet.

## III. THE ITU

### A. *The Early Beginnings*

In 1865, the International Telegraph Union was formed as a specialized body to find and develop international standards and provide needed technical assistance.[9] Globally, there was a recognized need for common rules to standardize equipment and to facilitate international interconnection.[10] In 1932, the International Radiotelegraph Union (IRU) and the International Telegraph Union formally merged, inheriting its current name, the International Telecommunications Union (ITU). In 1947 it became an agency under the UN. Although part of the UN system, it has exercised a significant amount of autonomy, having maintained an independent plenipotentiary body and Secretary General.

Since the founding of the ITU, the organization has had an important role in connecting national telecommunications networks together, establishing international telecommunications standards.[11] Experts within the ITU understand how telecommunications networks operate, allowing the ITU to serve the role as an effective broker between states over the years. The ITRs adopted in 1988 established general principles that were helpful in creating a framework for international cooperation for telegraph, radio and telephone communications.

### B. *Post 1988: Slipping Relevance*

Since 1988 and the intervening years leading up to WCIT-12, much had changed with international communications. Competitive and liberalized markets had emerged, national telecommunications service providers were privatized, and the Internet had flourished. In fact, some argued, the Internet had successfully developed so rapidly precisely because it operated without any formal international treaty, outside the overall direction of the ITU, through peer-to-peer relationships in "multi-stakeholder" forums like the IETF and ICANN. The ITU and the Internet technical community worked in parallel on related issues but in markedly different ways. The Internet's technical standards community held open working groups to develop and revise hundreds of new standards, making them available on-line for free. In contrast, the ITU's telecommunications standards development activities lacked transparency and had shrunk in size as its revenue model with high membership fees became increasingly unpopular. The ITU seemed to be slipping into irrelevance as the Internet thrived outside of its purview.

In the face of the evolution of international communications, the ITU was forced to reevaluate its role in regulating communications, looking for an overarching role in the regulation of the Internet lest it slip further into irrelevance. To do so, however, the organization would need to deviate from its past practice of concentrating on its core technical missions and shying away from political issues, launching the organization into entanglements with contentious political issues.

### C. *Post 1988: World Summit on the Information Society*

By the early 2000s, while ITU member states had not achieved consensus on what action should be taken since the emergence of the Internet, the issue was ripe for discussion. In 2002 the UN General Assembly approved the establishment of a two-phased World Summit on the Information Society (WSIS), identifying the need for enhancing the role of other governments in Internet governance. The WSIS effort would be led by the ITU, securing a future role for the ITU in

[7] Hamadoun Toure, Welcome Remarks to the Telecommunications Standardization Advisory Group (January 10, 2012). http://www.itu.int/en/osg/speeches/Pages/2012-01-10.aspx.

[8] CWG-WCIT12 Draft Information Document 7, Security in the use of ICTs, CWG-WCIT12/INF-7 (February 21, 2012) at 3.

[9] *See International Telegraph Conference (Paris, 1865)*, ITU History Portal, http://www.itu.int/en/history/plenipotentiaryconferences/Pages/1865Paris.aspx

[10] History of the ITU, http://www.itu.int/aboutitu/overview/history.html/

[11] For a history of the ITU, see George A. Codding, *The International Telecommunications Union: An Experiment in International Cooperation* (Brill, 1952)

Internet governance issues. In the Tunis Agenda for the Information Society, WSIS 2005, articles 68 and 69 made it explicit that Internet governance was going to be on the table for discussion in the future.[12]

In examining the resolutions adopted at the previous ITU plenipotentiary conferences, the emerging role of the ITU in the Internet space is revealed. Of note is resolution 102 from the November 2006 Antalya, Turkey Plenipotentiary Conference. The new language in the resolution expanded the ITU's role "with regard to international public policy issues pertaining to the Internet and the management of Internet resources."[13] By 2007 the ITU Secretary General had launched the Global Cybersecurity Agenda, formed a High Level Experts Group to develop advice on what the ITU could do with respect to cybersecurity and agreed to convene a WCIT in 2012 to consider the results of this review. The Internet-related resolutions from 2006 gave full acknowledgement to the WSIS, its results, and its implementation, with a key role for the ITU. The early debates during the WSIS process about the ITU's roles and responsibilities in relation to ICT and Internet governance were the initial steps in what would become a highly controversial issue over the ITU's appropriate role with respect to the Internet.

### D. *Post-Snowden: Renewed ITU Relevance Grab*

In June 2013, news stories of US' electronic intelligence-gathering capabilities began appearing in the media after Edward Snowden leaked classified information related to NSA's surveillance programs.[14] Since the disclosures were first made, the US has faced significant international outrage, negatively effecting US foreign relations. The escalating global controversy over the disclosures has given the ITU a renewed sense of focus as the organization appears poised to chart a new course for itself in matters of national security related to cyberespionage and cyberwarfare.

In a forthcoming publication, a former senior ITU official and secretary for the WCIT-12 preparatory process, Richard Hill, argues for additional ITU regulation of the Internet in light of the revelations, stating that without it there would be a "continuation of unilateral, and extraterritorial assertions of national powers, including surveillance and cyberwarfare" through the Internet.[15] In addition, the Brazilian President Dilma Rousseff, angered by disclosures that she had been subject to US surveillance, in a speech at the UN General Assembly, called for the establishment of "a civilian multilateral framework for the governance and use of the Internet."[16] While President Rousseff did not specifically mention the ITU, the former Brazilian president, in 2009, had suggested that the ITU should lead international cybersecurity coordination.[17]

There is no question that security issues related to the Internet are real and need international cooperative solutions. Effective solutions to these problems, however, will not come from ITU resolutions or recommendations. In fact, the proposals at WCIT-12 demonstrated just how ill-equipped the ITU is to handle cybersecurity matters that are linked to national security. The WCIT-12 proposals that related to spam, cybercrime and protecting the integrity and stability of data and networks were excessively vague, resulting in widely divergent assessments of the proposals' implications. The descriptions of the potential impact of the proposals ranged from 'meaningless, having no impact upon states' domestic authorities,' to 'highly dangerous, leading to ITU-directed state-dominated control over Internet content.'

The WCIT-12 controversy demonstrates why debates over the effectiveness of adapting specific organizations for specific new purposes are important. In this case, the security-related Internet matters of cybercrime and cybersecurity, that the ITU seeks to regulate involve more than network operations and ITU standards. Rather, they are intrinsically connected to states' national, international, military and political security. Challenges of such a complex nature go beyond the capabilities of the ITU. In the end, the current challenge with respect to the ITU is in determining when the limits of its institutional adaptation have been reached and when new policy challenges require the hard work of looking outside of this specific organization to get solutions.

## IV. ROLE OF INTERNATIONAL ORGANIZATIONS

### A. *Solving Common Problems*

International organizations (IOs) have never been more central to international politics than they are today. In the nineteenth century, as states faced the unprecedented international flow of commerce in goods, services, people, ideas, germs and social evils, a new type of international effort emerged. New international unions were created to help states solve problems with diverse characteristics, including technical, that the state did not have the capacity or desire to solve itself. Throughout the twentieth and into the twenty-first century these IOs grew in number and authority, establishing great power councils, universal conferences, specialized functional units and permanent staffs. The centralized structure of IOs allowed for the centralization of collective activities through a concrete and stable organizational structure and a supportive administrative apparatus.[18]

---

[12] WSIS, "Tunis Agenda for the Information Society," November 18, 2005; http://www.itu.int/wsis/docs2/tunis/off/6rev1.html.

[13] The Plenipotentiary Conference of the International Telecommunication Union, Resolution 102, "ITU's role with regard to international public policy issues pertaining to the Internet and the management of Internet resources, including domain names and addresses," (Antalya, 2006); http://www.itu.int/osg/csd/intgov/mandate/Res102.pdf.

[14] "New NSA leaks show how US is bugging its European allies," *The Guardian*, June 30, 2013; http://www.theguardian.com/world/2013/jun/30/nsa-leaks-us-bugging-european-allies.

[15] Richard Hill and Shawn Powers, "Cybersecurity and spam: WCIT and the future," IEEE (forthcoming).

[16] Julian Borger, "Brazilian president: US surveillance a 'breach of international law,'" *The Guardian*, Sept. 24, 2013; http://www.theguardian.com/world/2013/sep/24/brazil-president-un-speech-nsa-surveillance

[17] ITU Press Release at http://www.itu.int/newsroom/press_releases/2009/16.html.

[18] Kenneth Abbott & Duncan Snidal, "Why States Act through Formal International Organizations," JOURNAL OF CONFLICT RESOLUTION, vol. 42, pp. 3-32, 4 (1988).

The post WWII establishment of the United Nations and Bretton Woods was a continuation of the hope to institutionalize the aspirations of the "international community." As David Kennedy describes it, the "move to institutions" was a move from utopian aspirations to institutional accomplishment.[19] The move was an effort to replace empire with institutions that would promote the economic development of the colonized, end war through international dispute settlement, affirm human rights and other "community" goals through discourse, advance "democratic" governance, and codify and develop international rules.[20] From a liberal Wilsonian tradition view, IOs were seen as promoters of peace, engines of progress and agents of emancipation.

### B. *Challenging State Sovereignty*

However, as IOs proliferated to deal with a wide scope of issue areas, evolving in ways not intended by their creators, states struggled to maintain the balance between the benefits of IOs and the privileges of state sovereignty. States began to show reluctance to become involved in IOs, focusing more on their shortcomings as international bureaucracies that involved "costs of formal organization, and the irritations of IO autonomy."[21] In general, enthusiasm for IOs waned as more states found IOs to be unwilling "rule takers" instead of participants in a "pooling of sovereignty" for everyone's benefit.[22]

As IO officials and experts struggled within IOs to maintain this balance, international relations scholars turned their attention to the "messier" aspects of these organizations, documenting their many "pathologies."[23] The results of the studies illustrated important aspects of how IOs exercise power and how far their "good intentions can sometimes lead to unfortunate and tragic outcomes."[24]

The IOs regarded as having been the most successful in the Grotian approach of creating or enforcing ever more international law, like the WTO, became the subject of the most vocal complaints, on the grounds that they had done the most to undermine the power of states to govern themselves. States voiced concerns about the authority of IOs to bind states to rules that the state had not consented to. And while the recommendations of IOs were touted as mere "suggestions" or "opinion" and "advice," states came to understand them to be, in fact, more. IOs' recommendations were viewed as not just some "extra-legal phenomenon." Indeed, their non-binding resolutions and recommendations evolved into indications of what states think the law is.[25] These "suggestions" have "a significant independent legal effect" and can act as a moral, political or social force.[26] In addition, in framing the issues IOs are able to fix meanings to certain words that then can orient behavior of states,[27]as illustrated at WCIT-12 in the debate between states over the different meanings of words such as "information security" and "cybersecurity."

The on-going contest between the ITU and member states illustrates the challenges inherent in the emergence of IOs. As a body created by the cooperative efforts of states and dominated by national governments, the ITU is a typical IO established under international law. It is founded on a set of treaties dating back to 1865 that have binding force in international law – the ITU Constitution and Convention, the Radio Regulations, and the ITRs – as well as resolutions, recommendations and other non-binding instruments adopted by its conference.

As other IOs have, the ITU has a life of its own, redefining its missions as its original mandate is rendered outdated. As the ITU adapts to meet the challenges of the Internet, its normative reach will extend beyond what its creators had anticipated, "generating yet more regulatory imperatives to resolve the resulting potential conflicts."[28] This "mission creep" will ultimately result in problems developing between the ITU and other IOs at the "joints" between their respective "regime complexes," creating a need for the ITU to work out the problems, leading to more work and establishment of more rules by the ITU.[29] Allowing the ITU to extend its role into national security issues would create unnecessary conflict with the central work of the UN Security Council (UNSC) and the UN General Assembly (UNGA).

## V. APPROPRIATE APPROACHES TO CYBERESPIONAGE & CYBERWARFARE

### A. *International Venues*

In terms of international law, WCIT-12 involved attempts to bring Internet governance into a negotiated set of international rules. It made sense that given the differences over the years between states regarding Internet governance, some states would use the revision of the ITRs as an opportunity to use international law to advance their agendas on Internet governance, including what they perceive as security threats in this realm. Indeed, for those issues central to a state's security, including the Internet, international law does provide a mechanism for regulating state behavior.

For everyone concerned about cyberespionage and cyberwarfare, the appropriate venue for seeking consensus on

---

[19] David Kennedy, "The Move to Institutions," 8 CARDOZO L. REV. 841, 984-85 (1987).
[20] Id.
[21] Id. at 5.
[22] See e.g., Michael Barnett & Martha Finnemore, "The Power of Liberal International Organizations," in *Power in Global Governance* 182 (Michael Barnett & Raymond Duvall eds., 2005).
[23] Michael Barrett and Martha Finnemore, *Rules for the World: International Organizations in Global Politic*s, Cornell University Press (2004).
[24] Id. at 44.
[25] Frowein, *The Internal and External Effects of Resolutions by International Organziations*, ZaoRV 49 (1989).
[26] White, *The Law of International Organizations*, Manchester (1996), p. 93; Detter, *Law Making by International Organizations*, Stockholm (1965), p. 212.
[27] Barrett and Finnemore, pp. 32-34.
[28] Jose E. Alverez, "International Organizations: Then and Now," 100 AJIL 324, 328 (2006).
[29] See e.g., Kal Raustiala and David G. Victor, "The Regime Complex for Plant Genetic Resources," 58 INT'L ORG. 277, 279-80 (2004). For descriptions of various forms of "mission creep" among IOs and its consequences on relationships between IOs, see, for example, *The UN Security Council: From the Cold War to the 21st Century* 1-115 (David M. Malone ed., 2004); Jessica Einhorn, "The World Bank's Mission Creep," *Foreign Affairs*, Sept/Oct 2001, at 22.

a regulatory scheme for such state behavior is the UN but not under the auspices of Internet governance. Since the founding of the UN in 1945, the UNSC and the ICJ have carried out the function of settling disputes among states related to security issues. States' divergent views on issues of espionage and war in cyberspace will not be resolved based on the Internet numbering and naming resources. Nor will resolution come about from a discussion of the Internet Assigned Number Authority functions or the role of Internet connectivity providers and operators. Applying similar solutions for issues the ITU has managed in the past will not be effective in solving problems arising in radically different contexts. Resolution and international consensus related to these issues will reside within the mandates of organizations such as the UNSC, the UNGA and the ICJ.

B. *The Role of International Law*

The fundamental challenge for states grappling with issues of state behavior on the Internet is that the scope and manner of international law's applicability to such behavior has remained unsettled since the advent of the Internet. Indeed, at the time the current international legal norms emerged, the Internet was not a thought in the minds of those who drafted the relevant treaties or the states whose practice constituted customary law. State practice of cyber operations has outpaced the terms of the treaties and customary norms that have formed the basis of the governing legal regime.

For cyberespionage and cyberconflict, the question is whether existing international law applies to the Internet and, if so, which laws, how, and under the auspices of what international legal organization. Rightly, states have been concerned about this ambiguity especially given the recent reports of the Stuxnet operation against the Iran nuclear facility in Natanz, the cyberattacks against the oil company Saudi Aramco, allegations of Chinese cyber economic espionage against US companies, and, most recently, NSA's programs. In 2011, in recognition of the lack of clarity related to the controlling laws, the US published its *International Strategy for Cyberspace*[30] setting forth its position on the matter, stating, "Long-standing international norms guiding State behavior – in time of peace and conflict – also apply to cyberspace."[31] Most recently, UN members of the Group of Governmental Experts on Developments in the Field of International and Telecommunications in the Context of International Security (UNGGE), representing 15 states, including Russia, the US and China, agreed that the UN Charter principles and, more generally, international law, apply in cyberspace.[32]

C. *Jus ad Bellum & Jus in Bello*

Outside the parameters of the ITU and international telecommunications law, there are well-established international legal principles governing espionage and conflict that can be applied in the cyber domain.[33] This body of international law encompasses the norm of non-intervention; the *jus ad bellum*, the international law governing the resort to force by states; and the *jus in bello*, regulating the conduct of armed conflict. These laws are codified in treaty and customary international law established over years of state practice.

For those laws related to the recourse to the use of force, the UN Charter has set out the rules for using force and the principles of self-defense in articles 2(4) and 51, respectively. In addition, the customary principles of necessity and proportionality apply with any uses of force in self-defense. For those laws related to armed conflict, the Geneva and Hague conventions apply as well as customary principles of discrimination, proportionality and distinction. If treaty violations take place in these areas of international law there are dispute resolution mechanisms outlined in the treaties. If, for some reason, dispute settlement fails, the UN and the ICJ are authorized bodies to bring final resolution to the disputes.

D. *The UNSC*

Article 24 of the UN Charter gives the UNSC the primary responsibility for the maintenance of international peace and security and its decisions in this regard are binding on the all members of the UN.[34] In addition, the UN Charter gives the UNSC the authority and responsibility to "determine the existence of any threat to the peace, breach of the peace, or act of aggression,"[35] and recommend and lead responses thereto.[36] As Article 41 states, measures taken by the UNSC to restore peace could include, "complete or partial interruption of . . . postal, telegraphic, radio and other means of communication."[37] To date, the UNSC has not determined that a cyber operation can constitute a threat to the peace, breach of the peace, or act of aggression. There is no dispute, however, over the UNSC's authority to do so.

The international controversy over the NSA's programs is a question of whether and/or how the law should be changed or developed. Under international law, if a state believes that cyber activities, including espionage and conflict, conducted by another state constitutes unlawful intervention, use of force, or acts of aggression, arguments about the legality of such actions should be part of a discussion before an impartial decision-maker, one capable of making assessments about legality based on interpretation of relevant UN Charter provisions and state practice.

Over the 68 years since its formation, the UNSC has had occasion to address espionage and conflict between states.

---

[30] White House, "International Strategy for Cyberspace: Prosperity, Security, adn Openness in a Networked World," (May 2011); http://ww.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

[31] Id. at 9.

[32] UNGA Res. A/68/99, "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," June 24, 2013; http://www.un.org/ga/search/view_doc.asp?symbol=A/68/98&referer=http://www.un.org/disarmament/topics/informationsecurity/&Lang=E.

[33] *Tallinn Manual on the Intternational Law Applicable to Cyber Warfare* (Michael N. Schmitt, gen. ed., Cambridge University Press 2013), http://www.ccdcoe.org/249.; https://www.ccdcoe.org/249.html.

[34] UN Charter, Art. 24.

[35] Id., Art. 39.

[36] Id., Art. 41-49.

[37] Id., Art. 41.

The downing of the US U-2 surveillance plane, piloted by Francis G. Power, in Soviet territory in 1960 lead to a significant decision by the UNSC on the issue of espionage and international law.[38] In addition, the UNSC has ruled on a number of cases involving uses of force and armed conflict, to include the 1981 Israeli attack against the Osirak reactor in Iraq[39] and the 1991 Gulf War.[40] In these cases the UNSC grappled with the legality of decisions related state actions involving national security issues.

Even in the absence of a specific set of facts referencing particular acts that have or are about to occur, the UNSC could prohibit, in general, particular types of categories of cyber operations that would amount to a threat or breach to the peace as it has done in the case of international terrorism and the proliferation of weapons of mass destruction.[41]

E. *The ICJ*

The *Nicaragua* case is the most important decision by the ICJ on the substantive law on the use of force and armed conflict.[42] The ICJ relied on customary international law in ruling on issues of intervention, uses of force, armed attack and self-defense in the context of forcible interventions to help armed opposition forces.[43] The ICJ ruled that direct military intervention or indirect intervention through support for subversive activities in another state were wrongful in light of both the principle of non-use of force and that of non-intervention.

The case is also important as it raised issues about the ICJ's role, vis-à-vis the UNSC, in disputes concerning the use of force. The case demonstrated how the ICJ is limited in how far it renders decisions on matters related to questions of self-defense or aggression given that the UN Charter has given a special role to the UNSC. Although issues of the defined lines between the roles of the UNSC and the ICJ have still not been resolved, in practice, both of these IOs have been very capable of addressing issues of "high-politics" between states.

The UNSC and UNGA operate under the auspices of the UN Charter and, as such, are better suited to seek consensus on matters related to security issues over which the UN Charter controls. UNSC, the political organ with the primary responsibility of maintaining international peace and security, and the ICJ, the principal judicial organ of the UN, contribute to the maintenance of international peace and security by upholding the principles of the UN Charter and customary international law. Also, the UNSC has the enforcement mechanism to seek compliance with its mandate and resolutions. In conjunction with the UNSC, the ICJ could play a role in any dispute resolution process related to state behavior on the Internet as it has done over the years in other physical domains.

F. *The Role of States*

Given this tension between the UNSC and ICJ, the ICJ's unwillingness to make pronouncements on the legality of the use of force, and the seeming reluctance of the UNSC to do the same, it is very likely that in the context of cyber operations, answers to questions related to uses of force will be determined by states through their practice and agreement on the "rules of the road" in cyberspace. Through consent in some form, whether an international treaty, bi-lateral treaty or non-binding resolutions of one type or another, states will determine the future rules. The challenge will be formulating principles, capable of attracting a broad measure of agreement that apply, or ought to apply, to issues of intervention, use of force, and armed attack in cyberspace.

## VI. THE FUTURE PATH

The ITU is not an overarching umbrella organization with experience or jurisdiction to develop consensus between states on core national and international security issues related to the Internet. For issues related to espionage and warfare, consensus should be sought through state negotiations under direct UN auspices rather than a special IO like the ITU, established under a separate treaty focused on specific issues. Linking the diverse issues related to the Internet under the auspices of the ITU for convenience would be detrimental to the work of existing IOs and the development and application of international law.

The fact that espionage and conflict can now be waged through the Internet does not justify arguments for the ITU to take on the role of managing these activities for member states. Indeed, success for the ITU in expanding its boundaries into such security matters will entail "buying into" an unachievable mission, undermining the importance of its operational mission and creating conflicts with other IOs whose mandates directly cover such security matters. Calls for enlargement of the ITU's mandate will likely prove unsustainable as the ITU struggles to retain its legitimacy in the face of increased resistance from member states.

In October 2014, the ITU will host its Plenipotentiary conference in Korea to review its Constitution and Convention. It is likely that new controversial proposals by some member states will be raised at the conference seeking to expand the role of the ITU into cybersecurity areas related to espionage and cyber conflict. For the reasons stated in this article, the US should oppose any ITU intervention on issues related to cyberespionage and cyber conflict.

Outside the auspices of the ITU, states should energize their cyber diplomacy, leveraging like-minded states while seeking to include others, and accelerate cooperation on cybersecurity issues through international groups like the UNGGE. Alternatively, if the major state players fail to reach agreement on an appropriate multilateral international forum for states to debate the "rules of the road" for the Internet, states may view the ITU as the only option, however flawed.

---

[38] For a detailed discussion of the UNSC's position on the legality of the US U-2 espionage operations, see Quincy Wright, "Legal Aspects of the U-2 Incident," 54 AJIL 836 (1960).

[39] See W. Thomas Mallison & Sally V. Mallison, "The Israeli Aerial Attack of June 7, 1981, Upon the Iraqi Nuclear Reactor:Aggression or Self-Defense?," 15 VAND. J. TRANSNAT'L L. 417 (1982).

[40] Oscar Schachter, "United Nations Law in the Gulf War," 85 AJIL 452 (1991).

[41] See e.g., S.C. Res. 1371 (28 September 2001); S.C. Res. 1540 (28 April 2004).

[42] *Military and Paramilitary Activities in and against Nicaragu*a, ICJ Reports (1986) 14.

[43] Id. at 214, paras 206-208.